



115761

REPUBLIC OF  
GAMERS

# USER MANUAL

GT-AC2900

ROG Rapture Dual-band Gaming Router

ASUS

I15761

Prima edizione

Agosto 2019

## **INFORMAZIONI SUL COPYRIGHT**

Nessuna parte di questo manuale, compresi i prodotti e i software in esso descritti, può essere riprodotta, trasmessa, trascritta, archiviata in un sistema di recupero o tradotta in alcuna lingua, in alcuna forma e in alcun modo, fatta eccezione per la documentazione conservata dall'acquirente a scopi di backup, senza l'espressa autorizzazione scritta di ASUSTeK COMPUTER INC. ("ASUS").

ASUS FORNISCE QUESTO MANUALE "COSÌ COM'È" SENZA GARANZIA DI ALCUN TIPO, ESPLICITA O IMPLICITA, INCLUDENDO SENZA LIMITAZIONI LE GARANZIE O CONDIZIONI IMPLICITE DI COMMERCIALIZZABILITÀ O IDONEITÀ AD UN PARTICOLARE SCOPO. IN NESSUN CASO ASUS, I SUOI DIRIGENTI, FUNZIONARI, IMPIEGATI O DISTRIBUTORI SONO RESPONSABILI PER QUALSIASI DANNO INDIRETTO, PARTICOLARE, ACCIDENTALE O CONSEGUENTE (COMPRESI DANNI DERIVANTI DA PERDITA DI PROFITTO, PERDITA DI CONTRATTI, PERDITA D'USO O DI DATI, INTERRUZIONE DELL'ATTIVITÀ E SIMILI), ANCHE SE ASUS È STATA AVVISATA DELLA POSSIBILITÀ CHE TALI DANNI SI POSSANO VERIFICARE IN SEGUITO A QUALSIASI DIFETTO O ERRORE NEL PRESENTE MANUALE O NEL PRODOTTO.

I prodotti e nomi delle aziende che compaiono in questo manuale possono essere marchi registrati o diritti d'autore delle rispettive aziende, o meno, e sono usati a solo scopo identificativo o illustrativo, a beneficio dell'utente, senza alcuna intenzione di violazione dei diritti di alcun soggetto.

LE SPECIFICHE E LE INFORMAZIONI CONTENUTE IN QUESTO MANUALE SONO FORNITE A SOLO USO INFORMATIVO E SONO SOGGETTE A CAMBIAMENTI IN QUALSIASI MOMENTO, SENZA PREAVVISO, E NON POSSONO ESSERE INTERPRETATE COME UN IMPEGNO DA PARTE DI ASUS. ASUS NON SI ASSUME ALCUNA RESPONSABILITÀ E NON SI FA CARICO DI ALCUN ERRORE O INESATTEZZA CHE POSSA COMPARIRE IN QUESTO MANUALE COMPRESI I PRODOTTI E I SOFTWARE DESCRITTI AL SUO INTERNO.

Copyright © 2019 ASUSTeK Computer, Inc. Tutti i diritti riservati.

## **CONDIZIONI E LIMITI DI COPERTURA DELLA GARANZIA SUL PRODOTTO**

Le condizioni di garanzia variano a seconda del tipo di prodotto e sono specificatamente indicate nel Certificato di Garanzia allegato a cui si fa espresso rinvio.

Inoltre la garanzia stessa non è valida in caso di danni o difetti dovuti ai seguenti fattori: (a) uso non idoneo, funzionamento o manutenzione impropri inclusi (senza limitazioni) e l'utilizzo del prodotto con una finalità diversa da quella conforme alle istruzioni fornite da ASUSTeK COMPUTER INC. in merito all'idoneità di utilizzo e alla manutenzione; (b) installazione o utilizzo del prodotto in modo non conforme agli standard tecnici o di sicurezza vigenti nell'Area Economica Europea e in Svizzera; (c) collegamento a rete di alimentazione con tensione non corretta; (d) utilizzo del prodotto con accessori di terzi, prodotti o dispositivi ausiliari o periferiche; (e) tentativo di riparazione effettuato da una qualunque terza parte diversa dai centri di assistenza ASUSTeK COMPUTER INC. autorizzati; (f) incidenti, fulmini, acqua, incendio o qualsiasi altra causa il cui controllo non dipenda da ASUSTeK COMPUTER INC.; (g) abuso, negligenza o uso commerciale.



La Garanzia non è valida per l'assistenza tecnica o il supporto per l'utilizzo del Prodotto in merito all'utilizzo dell'hardware o del software. L'assistenza e il supporto disponibili (se previsti) nonché le spese e gli altri termini relativi all'assistenza e al supporto (se previsti) verranno specificati nella documentazione destinata al cliente fornita a corredo del prodotto. È responsabilità dell'utente, prima ancora di richiedere l'assistenza, effettuare il backup dei contenuti presenti sul Prodotto, inclusi i dati archiviati o il software installato. ASUSTeK COMPUTER INC. non è in alcun modo responsabile per qualsiasi danno, perdita di programmi, dati o altre informazioni archiviate su qualsiasi supporto o parte del prodotto per il quale viene richiesta l'assistenza; ASUSTeK COMPUTER INC. non è in alcun modo responsabile delle conseguenze di tali danni o perdite, incluse quelle di attività, in caso di malfunzionamento di sistema, errori di programmi o perdite di dati. È responsabilità dell'utente, prima ancora di richiedere l'assistenza, eliminare eventuali funzioni, componenti, opzioni, modifiche e allegati non coperti dalla Garanzia prima di far pervenire il prodotto a un centro servizi ASUSTeK COMPUTER INC. ASUSTeK COMPUTER INC. non è in alcun modo responsabile di qualsiasi perdita o danno ai componenti sopra descritti. ASUSTeK COMPUTER INC. non è in alcun modo responsabile di eliminazioni, modifiche o alterazioni ai contenuti presenti sul Prodotto compresi eventuali dati o applicazioni prodotte durante le procedure di riparazione del Prodotto stesso. Il Prodotto verrà restituito all'utente con la configurazione originale di vendita, in base alle disponibilità di software a magazzino.

### **LIMITAZIONE DI RESPONSABILITÀ**

Potrebbero verificarsi circostanze per le quali, a causa di difetti di componenti ASUS, o per altre ragioni, abbiate diritto a richiedere un risarcimento danni ad ASUS. In ciascuna di queste circostanze, a prescindere dai motivi per i quali si ha diritto al risarcimento danni, ASUS è responsabile per i danni alle persone (incluso il decesso), danni al patrimonio o alla proprietà privata; o qualsiasi altro danno reale e diretto risultante da omissione o mancata osservazione degli obblighi di legge previsti in questo Certificato di Garanzia, fino al prezzo contrattuale elencato per ogni prodotto e non oltre.

ASUS sarà solo responsabile o indennizzerà per perdite, danni o reclami su base contrattuale, extracontrattuale o di infrazione ai sensi del presente Certificato di Garanzia.

Questo limite si applica anche ai fornitori e rivenditori ASUS. Questo è il limite massimo per il quale ASUS, i suoi fornitori e il vostro rivenditore sono responsabili collettivamente.

IN NESSUN CASO ASUS È RESPONSABILE DI QUANTO SEGUE: (1) RICHIESTE DI TERZI PER DANNI DA VOI CAUSATI; (2) PERDITA O DANNEGGIAMENTO DEI VOSTRI DATI O DOCUMENTI O (3) QUALSIASI DANNO INDIRECTO, PARTICOLARE, ACCIDENTALE O CONSEGUENTE (COMPRESI DANNI DERIVANTI DA PERDITA DI PROFITTO, PERDITA DI CONTRATTI, PERDITA D'USO O DI DATI, INTERRUZIONE DELL' ATTIVITÀ E SIMILI) ANCHE SE ASUS, I SUOI DISTRIBUTORI E I VOSTRI RIVENDITORI SONO CONSAPEVOLI DELLA POSSIBILITÀ CHE TALI DANNI SI POSSANO VERIFICARE.

### **LICENZA SOFTWARE**

I prodotti ASUS possono essere corredati da software, secondo la tipologia del prodotto. I software, abbinati ai prodotti, sono in versione "OEM": il software OEM viene concesso in licenza all'utente finale come parte integrante del prodotto; ciò significa che non può essere trasferito ad altri sistemi hardware e che, in caso di rottura, di furto o in ogni altra situazione che lo renda inutilizzabile anche la possibilità di utilizzare il prodotto OEM viene compromessa. Chiunque acquisti, unitamente al prodotto, un software OEM è tenuto ad osservare i termini e le condizioni del contratto di licenza, denominato "EULA" (End User Licence Agreement), tra il proprietario del software e l'utente finale e visualizzato a video durante l'installazione del software stesso. Si avvisa che l'accettazione da parte dell'utente delle condizioni dell'EULA ha luogo al momento dell'installazione del software stesso.

### **ASSISTENZA E SUPPORTO**

Visitate il nostro sito all'indirizzo: <http://www.asus.com/it/support>

# Indice

<b>1</b>	<b>Conoscete il vostro router wireless</b>	
1.1	Benvenuti!.....	8
1.2	Contenuto della confezione.....	8
1.3	Assemblaggio del router .....	8
1.4	Il vostro router wireless .....	12
1.5	Posizionamento del router .....	14
1.6	Requisiti per l'installazione .....	15
<b>2</b>	<b>Per iniziare</b>	
2.1	Configurazione del router.....	16
	A. Connessione cablata .....	16
	B. Connessione senza fili .....	17
2.2	Installazione rapida Internet (QIS) con auto-rilevamento	19
2.3	Connessione alla vostra rete wireless.....	22
<b>3</b>	<b>Configurare le Impostazioni generali di ROG Gaming Center</b>	
3.1	Accedere all'interfaccia web.....	23
3.2	Dashboard .....	24
3.3	AiProtection Pro .....	28
	3.3.1 Configurazione di AiProtection Pro.....	29
	3.3.2 Blocco siti web malevoli.....	31
	3.3.3 IPS bidirezionale.....	32
	3.3.4 Prevenzione e blocco di dispositivi infetti.....	33
	3.3.5 Configurazione di Controllo Genitori .....	34
3.4	Accelerazione del gioco .....	37
	3.4.1 Accelerazione del gioco su tre livelli .....	38
	3.4.2 QoS.....	39
	3.4.3 Game Private Network .....	41

3.5	Open NAT .....	43
3.6	Game Radar.....	45
3.7	WiFi Radar .....	46
	3.7.1 Verifica sito Wi-Fi .....	47
	3.7.2 Statistiche canale wireless .....	48
	3.7.3 Risoluzione dei problemi avanzata .....	48
3.8	VPN .....	49
	3.8.1 VPN Fusion .....	50
3.9	Traffic Analyzer .....	52
<b>4</b>	<b>Configurare le Impostazioni avanzate</b>	
4.1	Usare la Mappa di rete .....	53
	4.1.1 Configurare le impostazioni di protezione della rete wireless .....	54
	4.1.2 Gestione dei client di rete .....	55
	4.1.3 Controllo del vostro dispositivo USB .....	56
	4.1.4 ASUS AiMesh .....	58
4.2	Wireless.....	64
	4.2.1 Generale .....	64
	4.2.2 WPS .....	66
	4.2.3 Bridge .....	68
	4.2.4 Filtro MAC wireless.....	70
	4.2.5 Impostazioni RADIUS.....	71
	4.2.6 Professionale .....	72
4.3	Creare una Rete ospiti.....	76
4.4	LAN .....	78
	4.4.1 LAN IP .....	78
	4.4.2 Server DHCP .....	79
	4.4.3 Rotte.....	81
	4.4.4 IPTV.....	82



4.5	WAN.....	83
4.5.1	Connessione ad Internet .....	83
4.5.2	WAN duale.....	86
4.5.3	Port Trigger.....	87
4.5.4	Virtual Server / Port Forwarding.....	89
4.5.5	DMZ.....	92
4.5.6	DNS Dinamico.....	93
4.5.7	NAT Passthrough.....	94
4.6	Utilizzare le Applicazioni USB .....	95
4.6.1	Usare AiDisk .....	96
4.6.2	Usare Gestione Server.....	98
4.6.3	3G/4G.....	103
4.7	Utilizzo di AiCloud 2.0.....	104
4.7.1	Disco Cloud.....	105
4.7.2	Smart Access.....	107
4.7.3	AiCloud Sync.....	108
4.8	IPv6.....	109
4.9	Firewall.....	110
4.9.1	Generale.....	110
4.9.2	Filtro URL.....	110
4.9.3	Filtro Parole Chiave .....	112
4.9.4	Packet Filter.....	113
4.10	Amministrazione.....	114
4.10.1	Modalità operativa.....	114
4.10.2	Sistema.....	115
4.10.3	Aggiornamento firmware .....	116
4.10.4	Ripristina/Salva/Carica Impostazioni.....	117
4.11	Registro di sistema .....	118
4.12	Smart Connect.....	119
4.12.1	Configurazione di Smart Connect.....	119
4.12.2	Regole di Smart Connect.....	120

## **5 Utility**

5.1	Device Discovery.....	123
5.2	Firmware Restoration.....	124
5.3	Impostare il server di stampa.....	125
5.3.1	ASUS EZ Printer Sharing.....	125
5.3.2	Utilizzo di LPR per condividere una stampante.....	129
5.4	Download Master.....	134
5.4.1	Impostazioni Torrent.....	135
5.4.2	Impostazioni NZB.....	136

## **6 Risoluzione dei problemi**

6.1	Risoluzione dei problemi più comuni.....	137
6.2	Domande frequenti (FAQ).....	139

## **Appendice**

Comunicazioni.....	148
Contatti ASUS.....	155

# 1 Conoscete il vostro router wireless

## 1.1 Benvenuti!

Vi ringraziamo per aver acquistato il router senza fili ROG Rapture! Questo router, molto sottile ed elegante, è dotato di due bande wireless, una a 2.4Ghz e l'altra a 5Ghz, per prestazioni impareggiabili negli streaming HD wireless, nei server Samba, UPnP AV e FTP per la condivisione di file 7 giorni su 7, 24 ore su 24. Il router inoltre è in grado di gestire fino a 300000 sessioni ed è stato progettato secondo la ASUS Green Network Technology per un risparmio di energia fino al 70%.

## 1.2 Contenuto della confezione

- |   |   |
|---|---|
| <input checked="" type="checkbox"/> Router wireless GT-AC2900                   | <input checked="" type="checkbox"/> 3 x Antenne wireless          |
| <input checked="" type="checkbox"/> Adattatore AC                               | <input checked="" type="checkbox"/> Cavo di rete Ethernet (RJ-45) |
| <input checked="" type="checkbox"/> Guida rapida                                | <input checked="" type="checkbox"/> 1 x Cacciavite                |
| <input checked="" type="checkbox"/> Dispositivo per supporto/montaggio a parete |   |

---

### NOTE:

- Nel caso in cui uno di questi articoli sia danneggiato, o mancante, contattate ASUS per ottenere supporto. Fate riferimento alle Hotline telefoniche ASUS che trovate in fondo a questo manuale.
  - Conservate la confezione originale integra nel caso abbiate bisogno, in futuro, di servizi di garanzia come la riparazione o la sostituzione.
- 

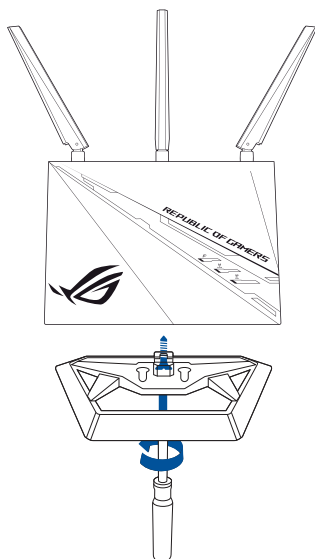
## 1.3 Assemblaggio del router

Grazie al piedistallo multi funzione il router GT-AC2900 garantisce massima flessibilità, potete decidere di installare il router su un tavolo o appenderlo al muro.



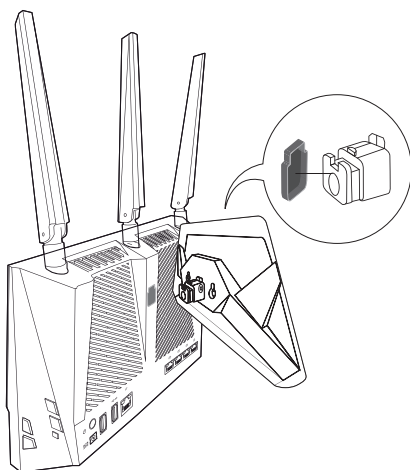
## Installazione su una superficie:

Posizionate il piedistallo multi funzione al di sotto del router, allineate la protrusione alla cavità, quindi serrate la vite.

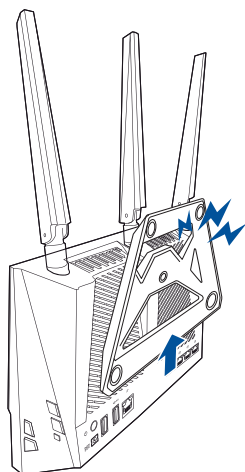


## Installazione a parete:

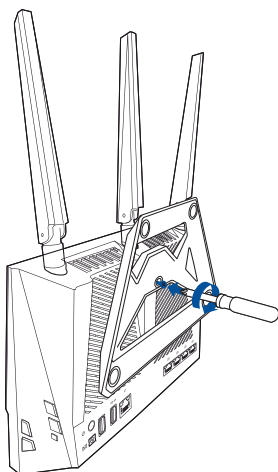
1. Posizionate il piedistallo multi funzione sul retro del router, quindi allineate la protrusione alla cavità.



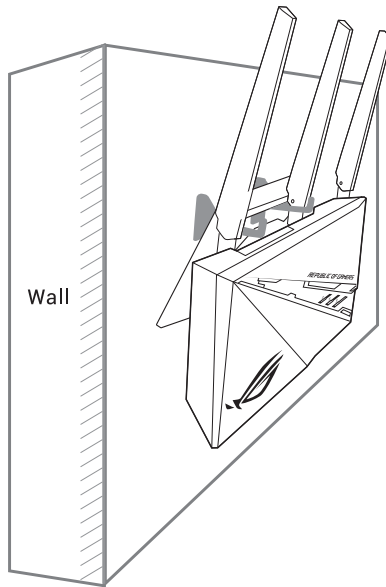
2. Spingete il piedistallo verso l'alto fino a quando sentite un clic.



3. Serrate la vite.



4. Fissate il router alla parete con tasselli e viti.



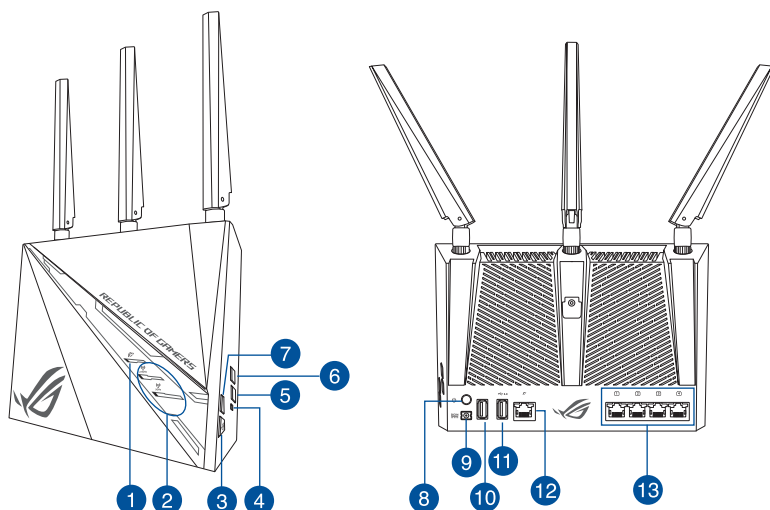
---

**Nota:** Assicuratevi che ciascun tassello sia fissato con una vite, e che sia in grado di sostenere almeno 2 kg di peso, per evitare che il router cada dalla sua posizione. I tasselli non sono inclusi nella confezione.

---



## 1.4 Il vostro router wireless



- 
- 1 LED Internet (WAN)**  
**Spento:** Nessuna connessione fisica.  
**Acceso:** Connessione fisica alla rete Internet (WAN).
- 
- 2 LED Wi-Fi 2.4GHz / 5GHz**  
**Spento:** Nessun segnale 2.4GHz o 5GHz.  
**Acceso:** Il sistema wireless è pronto.
- 
- 3 Tasto ROG Boost**  
Premete questo pulsante per modificare gli effetti di illuminazione Aura o attivare/disattivare Game Boost, Canale DFS e GeForce Now QoS.
- 
- 4 Pulsante di reset**  
Questo pulsante serve a ripristinare le impostazioni predefinite di fabbrica.
- 
- 5 Pulsante Wi-Fi**  
Premete questo pulsante per attivare o disattivare la rete Wi-Fi.
- 
- 6 Pulsante WPS**  
Questo pulsante attiva la configurazione guidata di WPS.
- 
- 7 Pulsante retroilluminazione**  
Premete questo pulsante per attivare o disattivare l'illuminazione Aura.
-

<b>8</b>	<b>Pulsante di accensione/spegnimento</b> Premete questo pulsante per accendere o spegnere il sistema.
<b>9</b>	<b>Porta ingresso alimentazione (DC-IN)</b> Inserite l'alimentatore in dotazione in questo ingresso e collegate il router ad una sorgente di alimentazione.
<b>10</b>	<b>Porta USB 2.0</b> In questa porta USB 2.0 potete inserire hard disk USB o memorie flash USB 2.0.
<b>11</b>	<b>Porta USB 3.0</b> In questa porta USB 3.0 potete inserire hard disk USB, memorie flash USB o una stampante.
<b>12</b>	<b>Porta Internet (WAN)</b> Collegate un cavo di rete in questa porta per stabilire una connessione WAN.
<b>13</b>	<b>Porte LAN</b> Collegate i cavi di rete in queste porte per stabilire connessioni LAN.

#### NOTE:

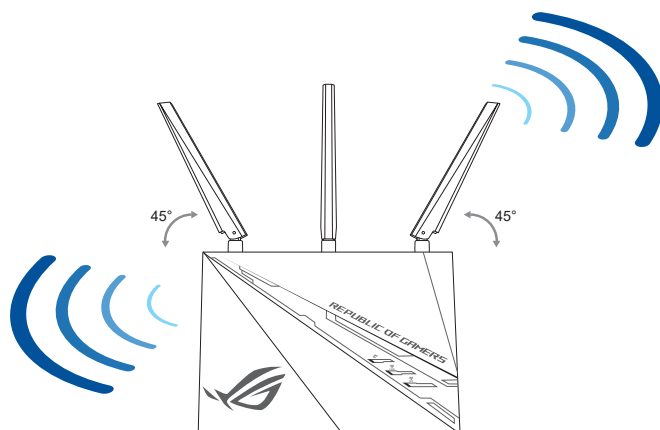
- Usate solamente l'adattatore di alimentazione che trovate nella confezione. L'utilizzo di altri adattatori potrebbe danneggiare il dispositivo.
- Posizionate il router in un ambiente asciutto e privo di temperature estreme. L'utilizzo all'esterno o calore eccessivo potrebbero generare pericoli.
- **Specifiche:**

<b>Adattatore di alimentazione DC:</b>	Uscita alimentatore DC: +19V con corrente massima 1.75A		
<b>Temperatura di esercizio</b>	0~40°C	<b>Archiviazione</b>	0~70°C
<b>Umidità di esercizio</b>	50~90%	<b>Archiviazione</b>	20~90%

## 1.5 Posizionamento del router

Per ottenere una migliore trasmissione del segnale tra il router wireless e i dispositivi di rete:

- Posizionate il router wireless il più possibile al centro della vostra area per avere una copertura globale migliore.
- Tenete il router lontano da ostacoli di metallo e dalla luce solare diretta.
- Tenete lontano da dispositivi Wi-Fi (che supportino solo 802.11g o 20Mhz), periferiche per computer a 2.4Ghz, dispositivi Bluetooth, telefoni cordless, trasformatori, motori pesanti, luci fluorescenti, forni a microonde, frigoriferi o altre attrezzature industriali per prevenire interferenze sul segnale.
- Aggiornate sempre all'ultimo firmware disponibile. Scaricate l'ultimo firmware disponibile dal sito web ASUS: <http://www.asus.com>.
- Posizionate il router in orizzontale.





## 1.6 Requisiti per l'installazione

Per configurare la vostra rete wireless avete bisogno di un computer che abbia almeno le seguenti caratteristiche:

- Porta (LAN) Ethernet RJ-45 (10Base-T/100Base-TX/1000Base-TX)
- Connettività wireless IEEE 802.11 a/b/g/n/ac/ax
- Protocollo TCP/IP installato sul sistema operativo
- Un browser Internet come Internet Explorer, Mozilla Firefox, Safari o Google Chrome

---

### NOTE:

- Se il vostro computer non è dotato di connettività wireless potete installare un adattatore WLAN, compatibile con gli standard IEEE 802.11 a/b/g/n/ac/ax, per connettervi alla rete wireless.
  - Grazie alla tecnologia dual-band il vostro router senza fili supporta simultaneamente i segnali wireless a 2.4GHz e 5GHz. Questo permette, prima di tutto, di svolgere attività su Internet come navigazione o lettura/scrittura di email usando la banda a 2.4Ghz e, allo stesso tempo, la trasmissione di file audio/video ad altra definizione (come filmati o musica) usando la banda a 5Ghz.
  - Alcuni dispositivi IEEE 802.11n che volete connettere alla rete potrebbero non essere compatibili con lo standard a 5Ghz. Fate riferimento al manuale utente del dispositivo per le specifiche.
  - Il cavo Ethernet RJ-45, usato per la connessione cablata, non deve essere lungo più di 100m.
-

## 2 Per iniziare

### 2.1 Configurazione del router

#### IMPORTANTE!

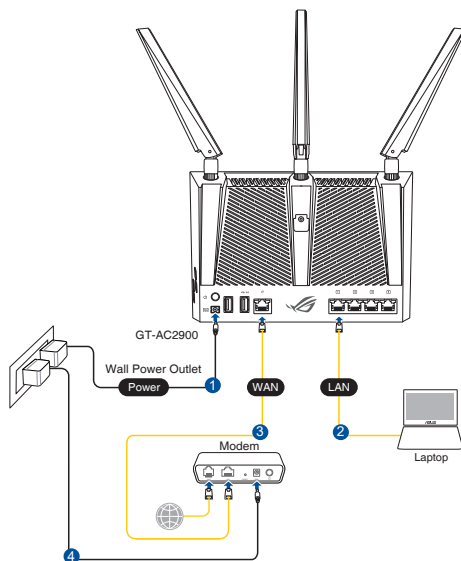
- Per evitare possibili problemi di configurazione consigliamo di usare una connessione cablata durante la configurazione del router wireless.
- Prima di configurare il vostro router wireless ASUS seguite questi semplici passaggi:
- Se state sostituendo un router esistente scollegatelo dalla rete.
- Scollegate i cavi che sono al momento collegati al modem. Se il modem ha una batteria supplementare rimuovete anche quella.
- Riavviate il vostro modem e il computer (raccomandato).

#### A. Connessione cablata

**NOTA:** Potete usare un cavo dritto, o incrociato (crossover), per la connessione cablata del PC al router.

#### Per configurare il vostro router wireless tramite una connessione cablata:

1. Collegate il router ad una presa di corrente e accendetelo. Collegate un cavo di rete dal vostro computer ad una porta LAN del router.



2. L'interfaccia web (GUI) si avvia automaticamente quando aprirete un browser web. In caso contrario inserite <http://router.asus.com> nella barra degli indirizzi
3. Impostate una password per il vostro router per prevenire accessi non autorizzati.

**Login Information Setup**

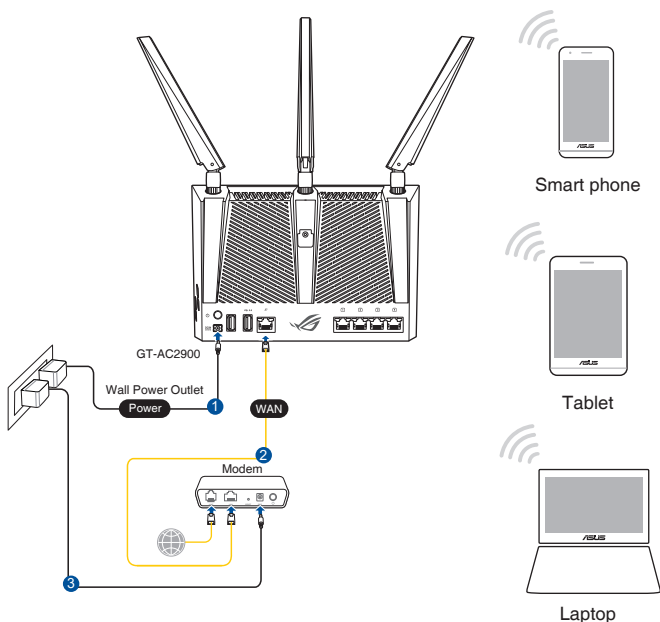
Change the router password to prevent unauthorized access to your ASUS wireless router.

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

## B. Connessione senza fili

**Per configurare il vostro router wireless tramite una connessione wireless:**

1. Collegate il router ad una presa di corrente e accendetelo.



2. Stabilite la connessione alla rete senza fili con nome (SSID) che trovate sull'etichetta nella parte posteriore del router. Per una migliore sicurezza di rete modificate il SSID inserendo un nome unico e assegnate una password.



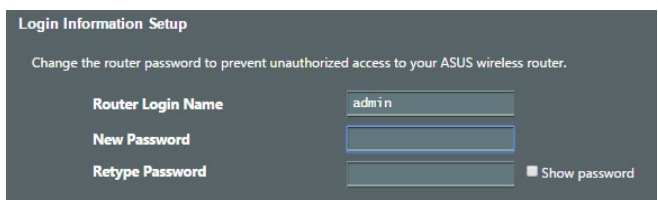
SSID predefinito: ASUS\_XX

\* **XX** corrisponde alle ultime due cifre dell'indirizzo MAC. Potete trovarlo sull'etichetta nella parte inferiore del router ROG.

- Una volta eseguita la connessione l'interfaccia web (GUI) si avvia automaticamente quando aprite un browser web. In caso contrario inserite <http://router.asus.com> nella barra degli indirizzi.
- Impostate una password per il vostro router per prevenire accessi non autorizzati.

**NOTE:**

- Per maggiori informazioni sulla connessione ad una rete wireless fate riferimento al manuale fornito con il vostro adattatore WLAN.
- Per sapere come configurare le impostazioni di sicurezza della vostra rete wireless fate riferimento alla sezione «Configurare le impostazioni di protezione della rete wireless» del Capitolo 3 di questo manuale.



## 2.2 Installazione rapida Internet (QIS) con auto-rilevamento

L'Installazione rapida Internet (QIS) vi aiuterà nella configurazione della vostra connessione a Internet.

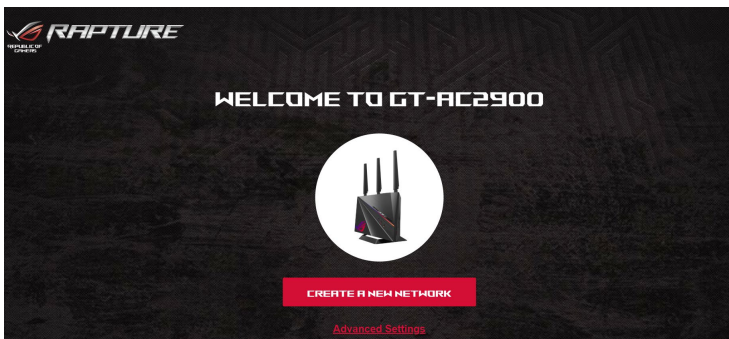
---

**NOTA:** Prima di impostare la connessione ad Internet per la prima volta assicuratevi di aver premuto il pulsante di Reset per riportare il router wireless alle impostazioni predefinite di fabbrica.

---

### Per usare l'auto-rilevamento dell'installazione rapida:

1. Avviate un browser web. Verrete reindirizzati ad ASUS Setup Wizard (Installazione rapida Internet o QIS). In caso contrario inserite <http://router.asus.com> manualmente.



2. Il router è in grado di capire automaticamente se la connessione fornita dal vostro ISP è a **IP dinamico**, **PPPoE**, **PPTP** o **L2TP**. Inserite le informazioni necessarie per individuare il tipo di connessione fornita dal vostro ISP.

---

**IMPORTANTE!** Ottenete le informazioni necessarie sul tipo di connessione dal vostro ISP.

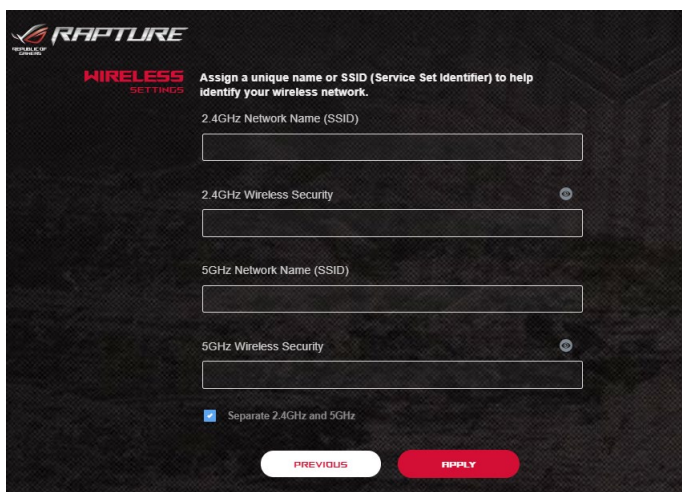
---

---

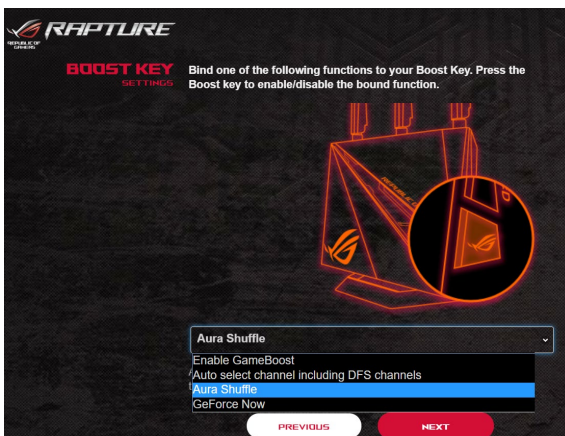
## NOTE:

- Il rilevamento automatico dell'ISP viene attivato quando configurate il router wireless per la prima volta, o dopo aver resettato il router wireless alle impostazioni di fabbrica.
  - Se l'installazione rapida Internet (QIS) fallisse cliccate su **Skip to manual setting (Configurazione manuale)** per configurare manualmente le impostazioni per la connessione ad Internet.
- 

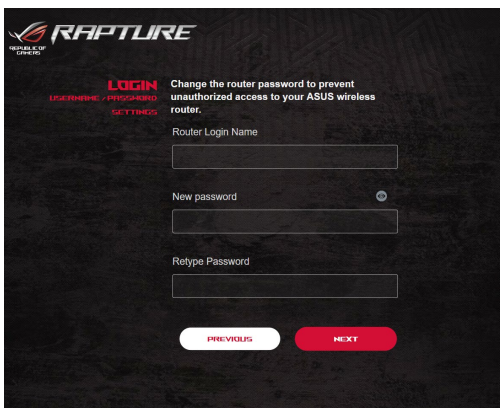
3. Impostate un nome della rete (SSID) e una chiave di sicurezza per le vostre reti wireless a 2.4GHz e 5GHz. Quando avete finito cliccate su **Apply (Applica)**.



4. Selezionate la funzione preferita per il tasto Boost.
  - **Aura Shuffle:** Permette di cambiare l'effetto di illuminazione Aura premendo il tasto Boost.
  - **Canale DFS acceso/spento:** Utilizza canali 5GHz addizionali per una banda più ampia e minore interferenza.
  - **GeForce NOW acceso/spento:** Assegna priorità elevata ai dispositivi GeForce Now.
  - **Game Boost acceso/spento:** Assegna priorità elevata ai pacchetti di gioco.



5. Nella pagina **Configurazione informazioni di accesso** cambiate la password di accesso per prevenire accessi non autorizzati al vostro router wireless.



---



**NOTA:** Il nome utente e la password del router wireless sono diversi dai SSID e dalle chiavi di sicurezza delle reti wireless 2.4GHz/5GHz. Il nome utente e la password del router wireless vi permettono di accedere all'interfaccia web del router per configurare le impostazioni del router. Il nome rete (SSID) delle reti 2.4GHz/5GHz e le chiavi di sicurezza permettono ai dispositivi Wi-Fi di accedere e connettersi alle reti wireless 2.4GHz/5GHz.

---

## 2.3 Connessione alla vostra rete wireless

Dopo aver configurato correttamente il router wireless tramite l'installazione rapida Internet (QIS) potete connettere il vostro computer, o altri dispositivi mobili, alla vostra rete wireless.

### Per connettervi alla rete:

1. Sul vostro computer cliccate sull'icona di rete  nell'area di notifica per visualizzare le connessioni wireless disponibili.
2. Selezionate una rete wireless alla quale volete connettervi e cliccate su **Connect (Connetti)**.
3. Potrebbe essere richiesto l'inserimento di una chiave di sicurezza per connettersi ad una rete wireless protetta. Dopo averla inserita cliccate su **OK**.
4. Aspettate qualche secondo per permettere al computer di stabilire la connessione correttamente. A connessione avvenuta sarà visualizzato lo stato della connessione e l'icona di rete visualizzata sarà la seguente .

---

### NOTE:

- Fate riferimento ai capitoli successivi per maggiori dettagli su come configurare le diverse impostazioni della vostra rete wireless.
  - Fate riferimento al manuale utente del vostro dispositivo per sapere come connettervi correttamente alla vostra rete wireless.
-



## 3 Configurare le Impostazioni generali di ROG Gaming Center

### 3.1 Accedere all'interfaccia web

Il router gaming ROG Rapture è dotato di un'interfaccia web grafica altamente intuitiva (GUI) - ROG Gaming Center, questo vi permette un controllo totale sulla vostra rete grazie a informazioni di base come lo stato dei dispositivi connessi, valori di ping per server gaming in tutto il mondo e accesso istantaneo a tutte le fantastiche funzioni gaming.

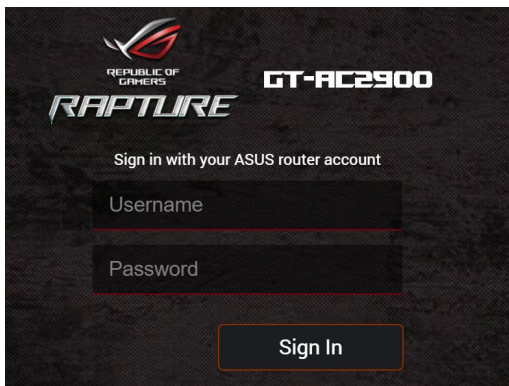
---

**NOTA:** Le caratteristiche possono variare in base alla versione del firmware installata sul router.

---

#### Per accedere all'interfaccia web GUI (Graphical User Interface):

1. Avviate il vostro browser e inserite, nella barra degli indirizzi, l'indirizzo standard del router: <http://router.asus.com>.
2. Nella pagina di accesso inserite il nome utente predefinito (**admin**) e la password che avete impostato in *2.2 Installazione rapida Internet (QIS) con auto-rilevamento*.



3. Ora potete usare la GUI per configurare le varie impostazioni del vostro router wireless ASUS.

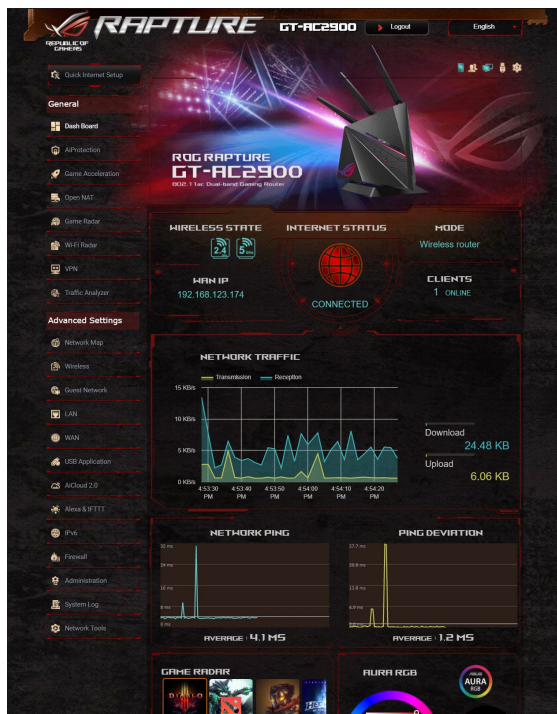
---

**NOTA:** Al primo accesso all'interfaccia web verrete indirizzati automaticamente all'installazione rapida Internet (QIS).

---

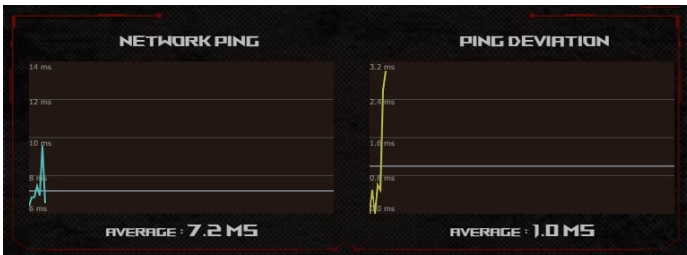
## 3.2 Dashboard

La Dashboard vi permette di monitorare il traffico in tempo reale per il vostro ambiente di rete e analizzare il ping in tempo reale e la deviazione del ping.

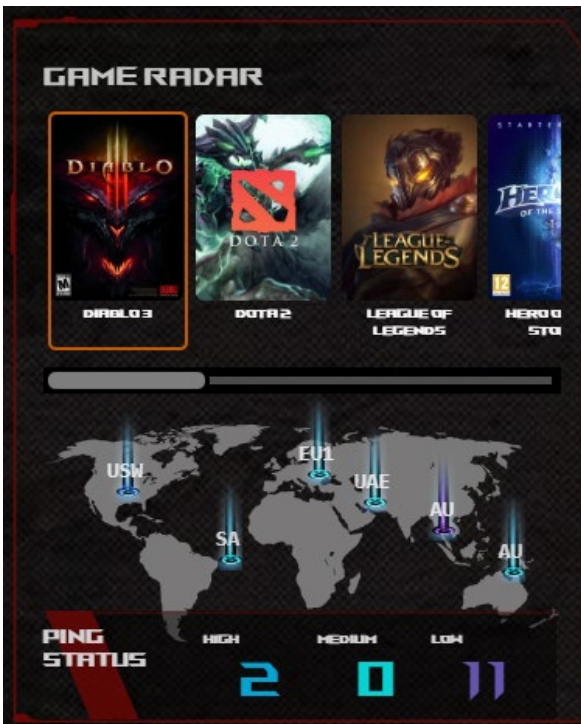


Il ping di rete è importante per le esperienze di gioco online. Un ping elevato si traduce in una latenza elevata per i giochi real-time. Per la maggior parte dei giochi online un ping di rete inferiore a 99 ms è considerato di buona qualità. Se il ping è inferiore a 150 ms la qualità è accettabile. In via generale se il ping è più elevato di 150 ms diventa difficile giocare con fluidità.

Anche la deviazione del ping è importante per le esperienze di gioco online. Con una deviazione del ping elevata è possibile andare incontro ad interruzioni durante il gioco online. Non c'è alcun criterio di base per la deviazione del ping. Tuttavia una deviazione del ping bassa è sempre preferibile.



- **Game Radar:** La funzione Game Radar può dare informazioni rapide sulla latenza di un server specifico.



- **Aura RGB:** Permette all'utente di configurare o attivare/disattivare la funzione Aura RGB. Potete impostare un qualsiasi colore e selezionare una tra le 11 modalità di illuminazione preimpostate.



- **Event Trigger**

Quando selezionate la modalità di illuminazione Event Trigger il sistema rileverà i seguenti eventi e ordinerà al LED di mostrare diversi effetti di illuminazione come notifica.

- **Game Boost**

Quando attivate Game Boost il LED lampeggia di rosso. Per ulteriori informazioni su Game Boost consultate la sezione «3.4 Accelerazione del gioco».

- **Contatore traffico**

Il LED multicolore mostra il traffico in tempo reale e cambia di colore a seconda della velocità Internet corrente.

- **Accesso fallito**

In caso di errore di accesso ad ASUSWRT, la barra LED si illumina con un effetto cometa di colore rosso.

- **Attacco bloccato**

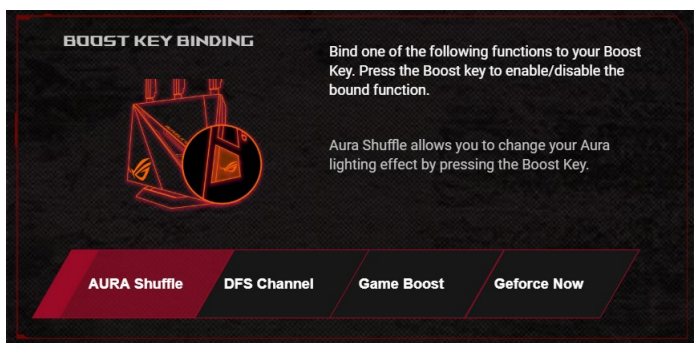
Quando il sistema blocca con successo un potenziale attacco il LED si illumina con un effetto cometa di colore rosso.

---

**Nota:** Una volta selezionata la modalità Event Trigger il sistema mostra diversi effetti di illuminazione a seconda degli eventi rilevati al momento. Se selezionate questa funzione non sarà possibile controllare gli effetti di illuminazione.

---

- **Tasto Boost:** Il router gaming ROG Rapture è dotato del tasto fisico Boost, configurabile in base alle esigenze dell'utente.



- **Aura Shuffle:** Permette di cambiare l'effetto di illuminazione Aura premendo il tasto Boost.
- **Canale DFS acceso/spento:** Utilizza canali 5GHz aggiuntivi per una banda più ampia e minore interferenza.
- **GeForce NOW acceso/spento:** Assegna priorità elevata ai dispositivi GeForce Now.
- **Game Boost acceso/spento:** Assegna priorità elevata ai pacchetti di gioco.

## 3.3 AiProtection Pro

AiProtection Pro fornisce monitoraggio in tempo reale per rilevare malware, spyware e accessi non autorizzati. Inoltre permette di filtrare siti web o app indesiderate e limitare l'accesso ad Internet ai dispositivi connessi per un determinato periodo di tempo.

**AiProtection**

*AiProtection with Trend Micro provides real-time network monitoring to detect malware, viruses, and intrusions before they can reach your PC or device. Parental Controls let you schedule times that a connected device is able to access the Internet. You can also restrict unwanted websites and apps.*

 **Network Protection**

- Router Security Assessment
- Malicious Sites Blocking
- Vulnerability Protection
- Infected Device Prevention and Blocking

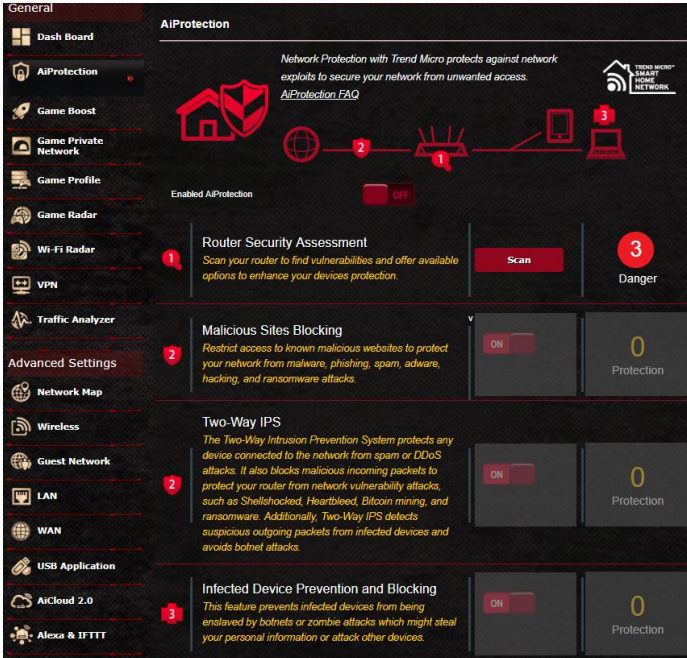
 **Parental Controls**

- Time Scheduling
- Web & Apps Filters



### 3.3.1 Configurazione di AiProtection Pro

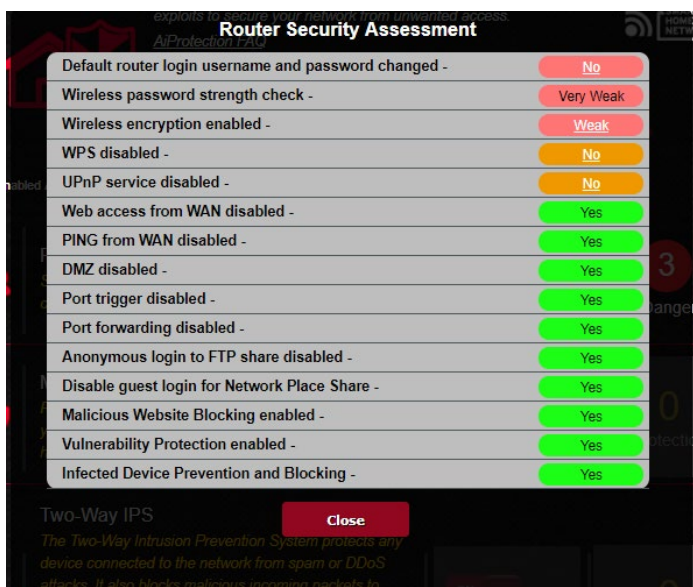
AiProtection Pro permette di proteggersi contro exploit di rete per impedire accessi non autorizzati.



**Per configurare AiProtection Pro:**

1. Dal pannello di navigazione andate su **General (Generale) > AiProtection Pro**.
2. Nella pagina principale di **AiProtection Pro** cliccate su **Network Protection (Protezione della rete)**.
3. Nella scheda di **Network Protection (Protezione della rete)** cliccate su **Scan (Scansione)**.

Una volta terminata la scansione verrete indirizzati alla pagina **Router Security Assessment (Valutazione della sicurezza del router)**.



**IMPORTANTE!** Le voci sicure vengono valutate con un **Yes (Sì)** nella pagina **Router Security Assessment (Valutazione della sicurezza del router)**.

4. (Opzionale) Nella pagina **Valutazione della sicurezza del router** configurate manualmente le voci valutate con **No**, **Debole** o **Molto debole**. Per fare questo:
  - a. Cliccate su una voce per accedere alle relative impostazioni.
  - b. Configurate e applicate le modifiche necessarie, cliccate su **Apply (Applica)** quando avete finito.
  - c. Tornate alla pagina **Valutazione della sicurezza del router** e cliccate su **Close (Chiudi)** per uscire.
5. Toccate **OK** al messaggio di conferma.



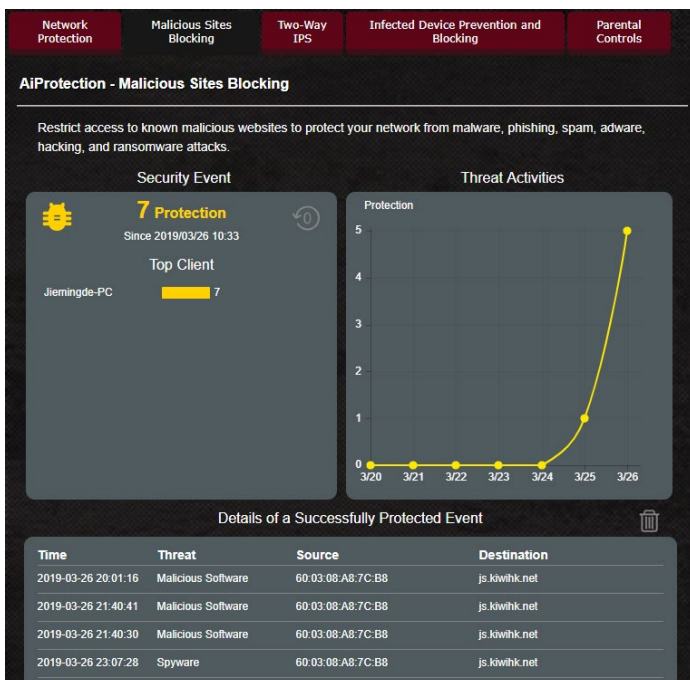
### 3.3.2 Blocco siti web malevoli

Questa funzione limita l'accesso ai siti web conosciuti, e dannosi, servendosi di un database cloud per una protezione sempre aggiornata.

**NOTA:** Questa funzione viene abilitata automaticamente se eseguite la **Router Weakness Scan (Scansione vulnerabilità del router)**.

#### Per abilitare Blocco siti web malevoli:

1. Dal pannello di navigazione andate su **General (Generale)** > **AiProtection Pro**.
2. Nella pagina principale di **AiProtection Pro** cliccate su **Network Protection (Protezione della rete)**.
3. Nel pannello di **Malicious Sites Blocking (Blocco siti web malevoli)** cliccate su **ON**.



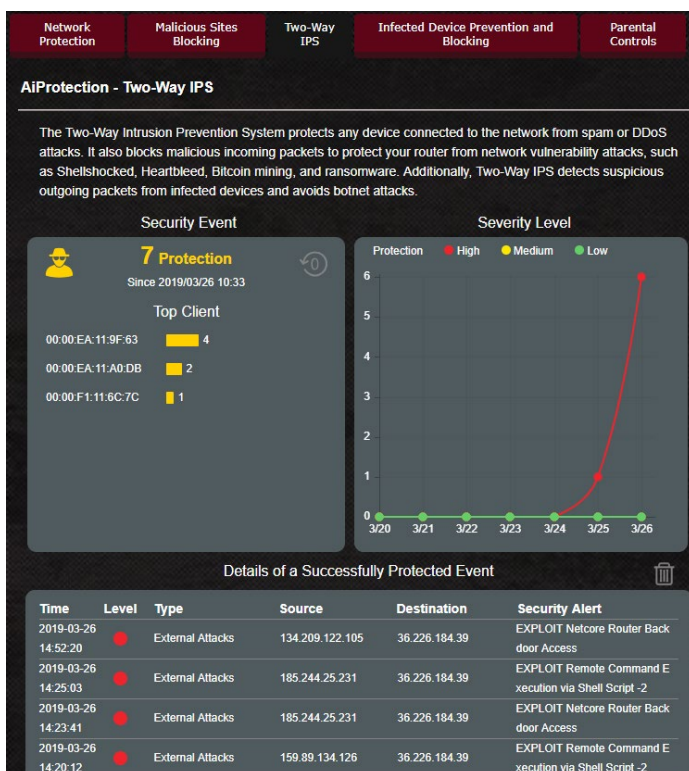
### 3.3.3 IPS bidirezionale

Questa funzione protegge contro gli exploit più comuni agendo sulla configurazione del router.

**NOTA:** Questa funzione viene abilitata automaticamente se eseguite la **Router Weakness Scan (Scansione vulnerabilità del router)**.

#### Per abilitare IPS bidirezionale:

1. Dal pannello di navigazione andate su **General (Generale) > AiProtection Pro**.
2. Nella pagina principale di **AiProtection Pro** cliccate su **Network Protection (Protezione della rete)**.
3. Nel pannello di **Two-Way IPS (IPS bidirezionale)** cliccate su **ON**.



### 3.3.4 Prevenzione e blocco di dispositivi infetti

Questa funzione impedisce ai dispositivi connessi infetti di diffondere informazioni personali, o informazioni di vulnerabilità, a soggetti esterni.

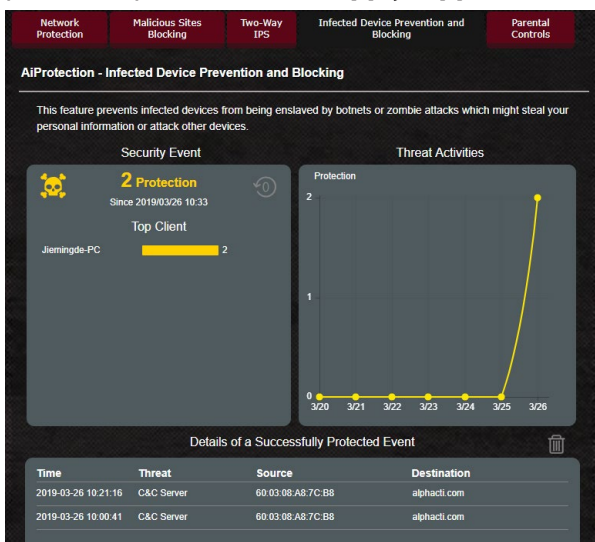
**NOTA:** Questa funzione viene abilitata automaticamente se eseguite la **Router Weakness Scan (Scansione vulnerabilità del router)**.

#### Per abilitare la prevenzione e il blocco di dispositivi infetti:

1. Dal pannello di navigazione andate su **General (Generale) > AiProtection Pro**.
2. Nella pagina principale di **AiProtection Pro** cliccate su **Network Protection (Protezione della rete)**.
3. Nel pannello di **Infected Device Prevention and Blocking (Prevenzione e blocco di dispositivi infetti)** cliccate su **ON**.

#### Per configurare Preferenze avvisi:

1. Nel pannello di **Infected Device Prevention and Blocking (Prevenzione e blocco di dispositivi infetti)** cliccate su **Alert Preference (Preferenze avvisi)**.
2. Selezionate o inserite il provider email, l'account email e la password quindi cliccate su **Apply (Applica)**.



### 3.3.5 Configurazione di Controllo Genitori

Controllo genitori permette di controllare l'orario di accesso ad Internet, o di impostare un tempo limite, per i clienti della rete.

#### Per abilitare Controllo Genitori:

1. Dal pannello di navigazione andate su **General (Generale)** > **AiProtection Pro**.
2. Nella pagina principale di **AiProtection Pro** cliccate su **Parental Controls (Controllo genitori)**.

**Network Protection**   **Malicious Sites Blocking**   **Two-Way IPS**   **Infected Device Prevention and Blocking**   **Parental Controls**

**AiProtection - Web & Apps Filters**   **Web & Apps Filters**   **Time Scheduling**

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

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

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

Web & Apps Filters   **ON**

**Client List (Max Limit : 16)**

<input type="checkbox"/>	Client Name (MAC Address)	Content Category	Add / Delete
<input type="checkbox"/>		<b>Adult</b> <i>Block adult/mature content to prevent children from visiting sites that contain material of a sexual, violent, and illegal nature.</i>	
<input type="checkbox"/>		<b>Instant Message and Communication</b> <i>Block instant communication software and messaging apps to prevent children from becoming addicted to social networking sites.</i>	
<input checked="" type="checkbox"/>	ex: 18:91:8F:89:26:E0	<b>P2P and File Transfer</b> <i>By blocking P2P and File Transferring you can make sure your network has a better quality of data transmission.</i>	
<input type="checkbox"/>		<b>Streaming and Entertainment</b> <i>By blocking streaming and entertainment services you can limit the time your children spend online.</i>	

## Filtro web e app

Filtro web e app è una funzione di Controllo genitori e permette di impedire l'accesso a siti web e app non desiderate.

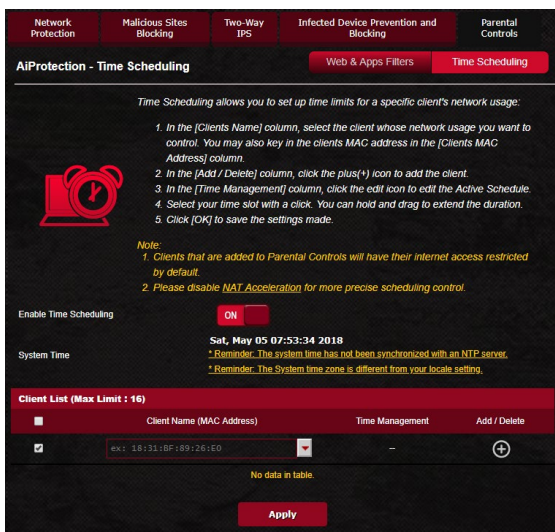
### Per configurare Filtro web e app:

1. Dal pannello di navigazione andate su **General (Generale)** > **AiProtection Pro**.
2. Nella pagina principale di **AiProtection Pro** cliccate sull'icona di **Parental Controls (Controllo Genitori)** per accedere alla scheda relativa.
3. Nel pannello di **Web & Apps Filters (Filtro web e app)** cliccate su **ON**.
4. Quando appare il messaggio con il contratto di licenza per l'utente finale (EULA) cliccate su **I agree (Accetto)** per continuare.
5. Nella colonna **Client List (Elenco client)** selezionate o inserite il nome del client.
6. Nella colonna **Content Category (Categoria di contenuti)** impostate il filtro per le quattro categorie principali: **Adulti, Chat e comunicazione, Trasferimento file e P2P e Intrattenimento**.
7. Cliccate su  per aggiungere il profilo del client.
8. Cliccate su **Apply (Applica)** per confermare le modifiche.

## Pianificazione temporale

Pianificazione temporale vi permette di impostare un limite di tempo per l'utilizzo della rete da parte di un client.

**NOTA:** Assicuratevi che l'ora di sistema sia sincronizzata con il server NTP.



### Per configurare Pianificazione temporale:

1. Dal pannello di navigazione andate su **General (Generale)** > **AiProtection Pro** > **Parental Controls (Controllo Genitori)** > **Time Scheduling (Pianificazione temporale)**.
2. Nel pannello di **Enable Time Scheduling (Abilita Pianificazione temporale)** cliccate su **ON**.
3. Nella colonna **Clients Name (Nome client)** selezionate o inserite il nome del client.

**NOTA:** Potete anche inserire l'indirizzo MAC nella colonna **Client MAC Address (Indirizzo MAC client)**. Assicuratevi che il nome del client non contenga caratteri speciali o spazi perché potreste causare un malfunzionamento del router.

4. Cliccate su **+** per aggiungere il profilo del client.
5. Cliccate su **Apply (Applica)** per confermare le modifiche.



## 3.4 Accelerazione del gioco

The screenshot displays the ASUS Game Acceleration settings page, organized into three levels of acceleration. The left sidebar contains navigation options under 'General' and 'Advanced Settings'. The main content area is titled 'Triple-level game acceleration' and includes a descriptive paragraph and three numbered sections.

**Game Acceleration** | QoS | WiFiST

**General**

- Dash Board
- AIProtection
- Game Acceleration**
- Open NAT
- Game Radar
- WiFi Radar
- VPN
- Traffic Analyzer

**Advanced Settings**

- Network Map
- Wireless
- Guest Network
- LAN
- WAN
- USB Application
- AICloud 2.0
- Alexa & IFTTT
- IPv6
- Firewall
- Administration
- System Log

### Triple-level game acceleration

Accelerate game traffic every step of the way from your device to the game server, ensuring the best connection and performance.

**LEVEL 1 Gaming Port Prioritization**

**LEVEL 2 Game Packet Prioritization**

**LEVEL 3 Game Server Acceleration**

### Gaming Port Prioritization

**Game Devices**

Dedicated gaming port that prioritizes network traffic to connected devices.

**ROG First** | FAQ

GameFirst V comes with ROG motherboards, laptops, and desktops to optimize network traffic for online PC gaming. By simply clicking ROG First in GameFirst V, your router will automatically recognize ROG devices and enable Level 2 acceleration.

**GO**

### Game Packet Prioritization

**Game Boost** | FAQ

Enable Game Boost:

Game Boost activates gaming mode using adaptive QoS. All gaming traffic passing through ROG routers can be prioritized to ensure ultimate gaming performance.

**GO**

### 3.4.1 Accelerazione del gioco su tre livelli

GT-AC2900 offre un'accelerazione del gioco su tre livelli per assicurare connessione e prestazioni migliori.

- **Priorità per la porta gaming**

Sarà sufficiente collegare il dispositivo di gioco alla porta gaming (GT-AC2900:LAN1) per ottenere priorità di traffico elevata.

**ROG First** è un'utility per schede madri ASUS ROG in **Game first V** e può essere usata in collaborazione con i router gaming ASUS ROG.

- **Priorità dei pacchetti di gioco**

Questa opzione vi permette di abilitare la funzione Game Boost con un click. Quando la funzione Game Boost è abilitata il router gaming ROG Rapture garantisce alta priorità ai pacchetti di gioco per fornirvi l'esperienza di gioco migliore possibile.

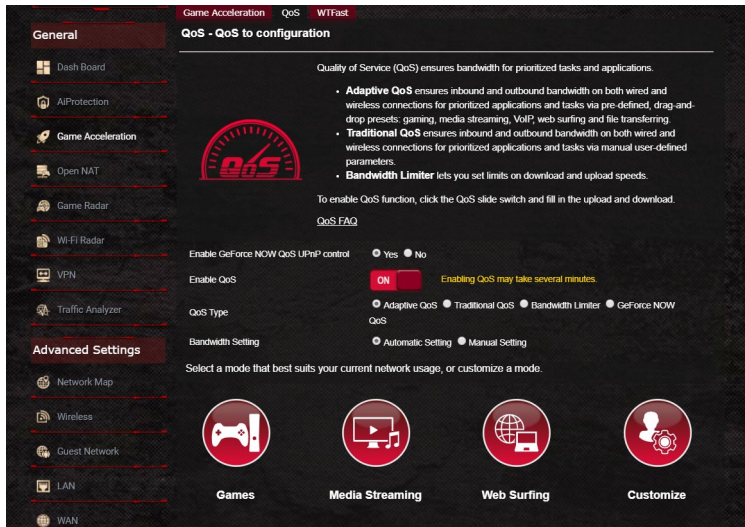
- **Accelerazione server di gioco**

La rete Gamers Private Network (GPNTM) fornita da WTFast riduce la latenza media di gioco e permette di diminuire picchi di flusso e perdita di pacchetti con la vostra connessione. Per ulteriori informazioni consulta la sezione «3.4.3 Game Private Network».



## 3.4.2 QoS

Questa funzione riserva una porzione di banda per applicazioni e processi più importanti.



### Per abilitare la funzione QoS:

1. Dal pannello di navigazione andate su **General (Generale)** > **Game Acceleration (Accelerazione del gioco)** e poi selezionate la scheda **QoS**.
2. Nel pannello di **Enable QoS (Abilita QoS)** cliccate su **ON**.
3. Specificate un valore per la banda in upload e download.

---

**NOTA:** Contattate il vostro ISP per ottenere i valori di banda disponibili con la vostra connessione. Se volete potete visitare il sito <http://speedtest.net> per verificare la vostra banda disponibile.

---

4. Selezionate il tipo di QoS (adattativo, tradizionale o limite banda) che volete utilizzare.

---

**NOTA:** Fate riferimento alla scheda QoS per la definizione della tipologia di QoS.

---

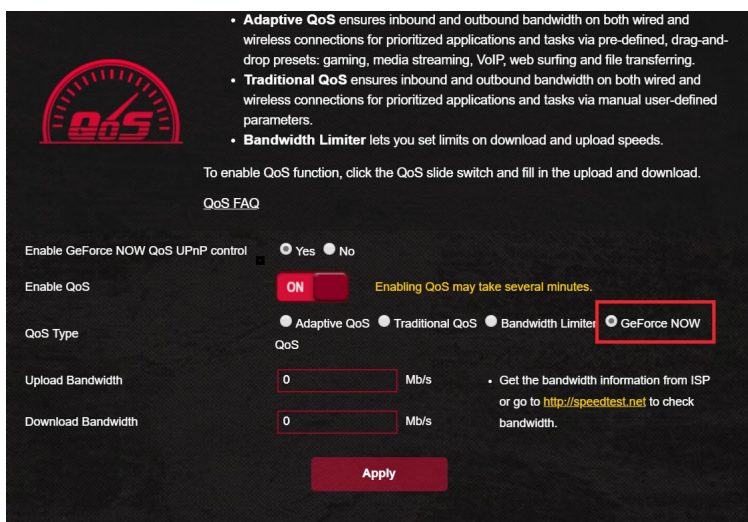
5. Cliccate su **Apply (Applica)**.

## GeForce NOW QoS

La modalità GeForce NOW QoS è specifica per i dispositivi compatibili GeForce NOW e i servizi gaming cloud NVIDIA (ad es. NVIDIA Shield TV). Abilitando la modalità GeForce NOW QoS il router riserverà banda richiesta, modalità senza fili e priorità QoS ai dispositivi abilitati GeForce NOW come stabilito da NVIDIA.

### Per abilitare GeForce NOW QoS:

1. Andate su **Game Acceleration (Accelerazione di gioco) > QoS**, cliccate sul pulsante **Enable QoS (Abilita QoS)** quindi selezionate la modalità QoS **GeForce NOW**.



- **Adaptive QoS** ensures inbound and outbound bandwidth on both wired and wireless connections for prioritized applications and tasks via pre-defined, drag-and-drop presets: gaming, media streaming, VoIP, web surfing and file transferring.
- **Traditional QoS** ensures inbound and outbound bandwidth on both wired and wireless connections for prioritized applications and tasks via manual user-defined parameters.
- **Bandwidth Limiter** lets you set limits on download and upload speeds.

To enable QoS function, click the QoS slide switch and fill in the upload and download.

QoS FAQ

Enable GeForce NOW QoS UPnP control  Yes  No

Enable QoS  **ON** Enabling QoS may take several minutes.

QoS Type  Adaptive QoS  Traditional QoS  Bandwidth Limiter  **GeForce NOW**

Upload Bandwidth  Mb/s

Download Bandwidth  Mb/s

Get the bandwidth information from ISP or go to <http://speedtest.net> to check bandwidth.

**Apply**

2. Enable GeForce NOW QoS UPnP control (Abilita GeForce NOW QoS UPnP control).  
Selezionate "**Yes (Si)**". La modalità GeForce NOW QoS si abilita automaticamente quando il router rileva dispositivi compatibili GeForce NOW.
3. Impostate la banda in upload/download desiderata. Per conoscere i valori di banda disponibili potete rivolgervi al vostro fornitore di servizi Internet (ISP) o usare uno dei vari strumenti disponibili online.
4. Cliccate su **Apply (Applica)** per salvare la configurazione.

### 3.4.3 Game Private Network

La rete Gamers Private Network (GPNTM) fornita da WTFast riduce la latenza media di gioco e permette di diminuire picchi di flusso e perdita di pacchetti con la vostra connessione. Potete godere di una connessione più veloce, fluida e reattiva con praticamente tutti i giochi di tipo MMO.



#### Per aggiornare il firmware:

1. Avviate il browser web e digitate <http://router.asus.com>, inserite nome utente e password predefinite (admin/admin) per accedere ad ASUSWRT GUI.
2. Andate su **Administration (Amministrazione) > Firmware Upgrade (Aggiornamento firmware)** e cliccate su **Check (Controlla)** quindi seguite le istruzioni sullo schermo per aggiornare il firmware.

Potete anche scaricare l'ultimo firmware disponibile dal sito <http://support.asus.com/ServiceHome.aspx> e poi aggiornare manualmente.

### Per usare WTFast:

1. Dal pannello di navigazione andate su **General (Generale)** > **Game Acceleration (Accelerazione del gioco)** > **WTFast**.
2. Create un account WTFast su <https://www.wtfast.com/>.
3. Eseguite l'accesso all'account WTFast.
4. Nell'elenco **WTFast Rules (Regole WTFast)** create un profilo per il dispositivo sul quale volete usare WTFast GPN.
5. Selezionate un server GPN in base alla vostra posizione o selezionate "Auto" e "Apply".
6. Abilitate il profilo GPN **PRIMA** di avviare il gioco.

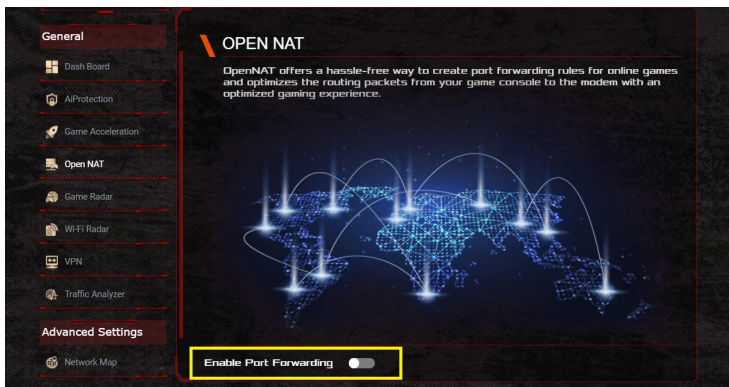
---

**NOTA:** L'account gratis supporta un solo dispositivo, se volete usare dispositivi multipli cliccate su **Upgrade** per sottoscrivere un abbonamento.

---

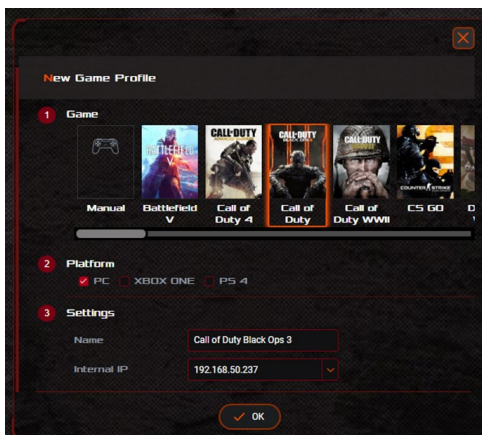
## 3.5 Open NAT

Quando giocate su console o PC potrebbero verificarsi alcuni problemi di connessione a causa del vostro ISP o di alcune impostazioni della vostra rete come NAT o blocco di alcune porte. Open NAT si assicura che il router gaming ROG Rapture non blocchi in alcun modo la connessione di gioco.

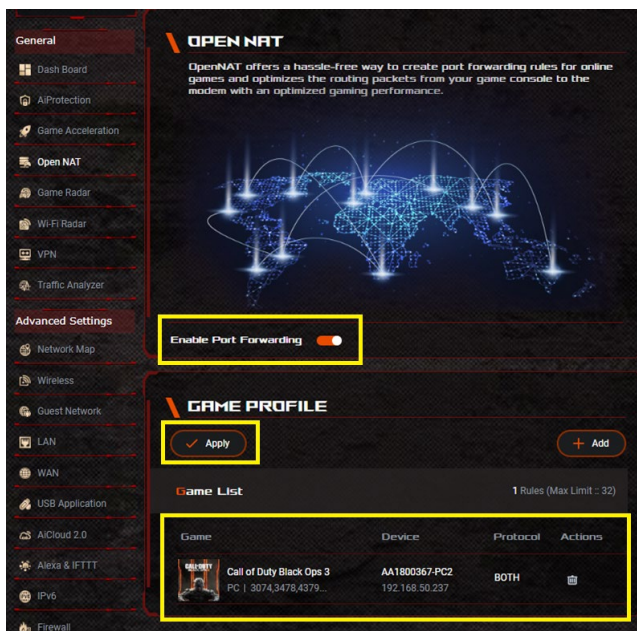


### Per usare Open NAT:


1. Dal pannello di navigazione andate su **General (Generale) > Open NAT** e abilitate la voce **Enable port forwarding (Abilita port forwarding)**.
2. Selezionate un gioco dall'elenco dei giochi, questo elenco viene aggiornato costantemente.

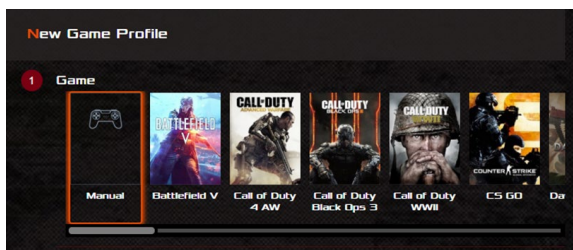


3. Selezionate la piattaforma che volete usare.
4. Nel campo Internal IP field (Indirizzo IP interno) inserite l'indirizzo IP del vostro dispositivo.
5. Cliccate su **OK** e poi su **Apply (Applica)**.



**Note:**

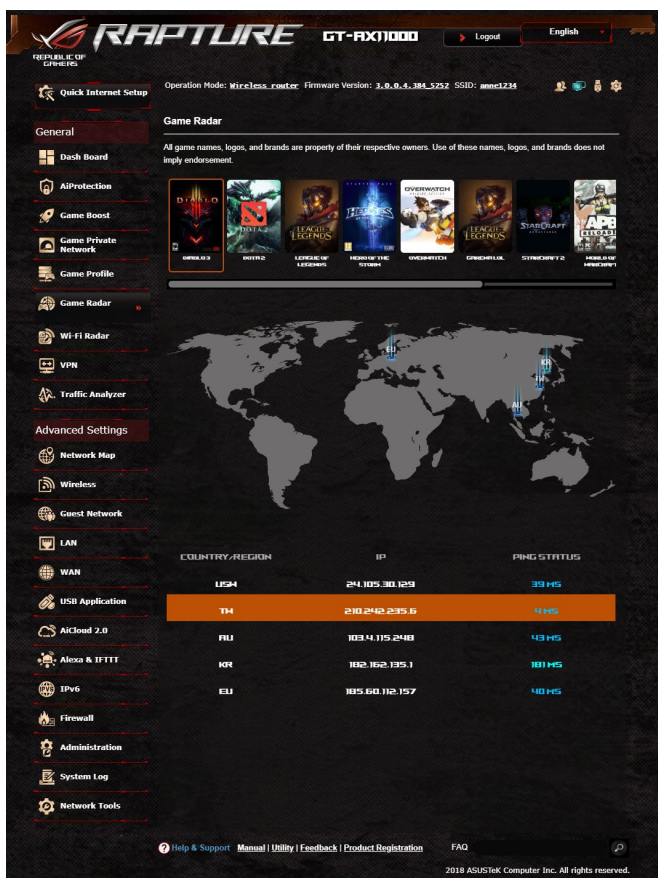
- Se volete configurare regole di port forwarding aggiuntive per il server FTP o altri servizi andate su WAN > Virtual server/Port Forwarding (vedi sezione 4.5.4).
- Se il vostro gioco non è incluso nei profili di gioco cliccate su  quindi selezionate **Manual (Manuale)** per creare una regola.





## 3.6 Game Radar

Game Radar è uno strumento di diagnostica che vi permette di identificare la qualità di connessione dei server per giochi specifici.



The screenshot shows the Rapture GT-RX1000 Game Radar interface. The top navigation bar includes the Rapture logo, the model name 'GT-RX1000', and a language dropdown set to 'English'. Below the navigation bar, the 'Game Radar' section is active, displaying a world map with server locations marked by blue pins. A table below the map lists the ping status for various countries and regions.

COUNTRY-REGION	IP	PING STATUS
USA	24.105.30.129	39 PMS
TH	210.240.235.6	11 PMS
RU	103.4.115.248	43 PMS
KR	102.162.135.1	101 PMS
EU	185.60.112.157	110 PMS

### Per usare Game Radar:

1. Dal pannello di navigazione andate su **General (Generale)** > **Game Radar** e selezionate un gioco dall'elenco.
2. Controllate il valore di **Ping Status (Durata ping)** per ciascun server.
3. Per un'esperienza di gioco fluida selezionate un server con ping basso.

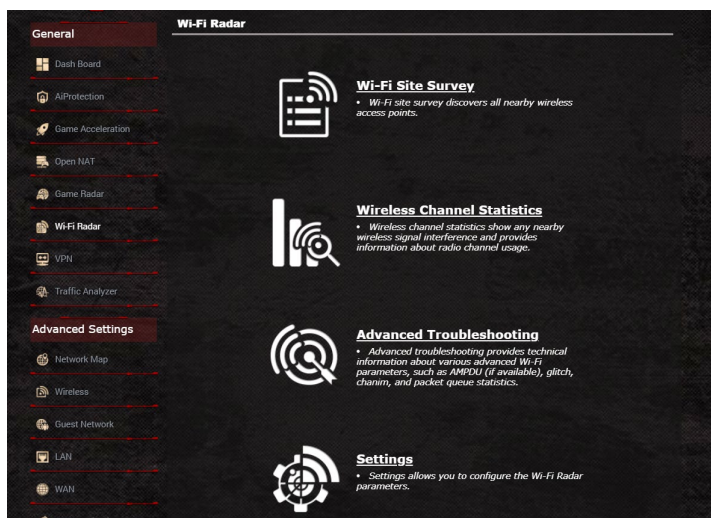
## 3.7 WiFi Radar

WiFi Radar, uno strumento avanzato per la vostra rete wireless, analizza a fondo i canali e i pacchetti trasferiti per una risoluzione dei problemi avanzata.

---

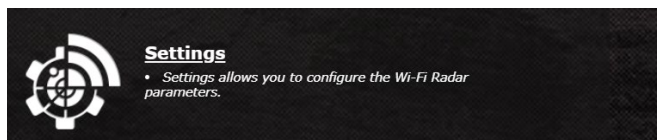
**NOTA:** Abilitare WiFi Radar potrebbe causare un peggioramento delle prestazioni wireless. Abilitate WiFi Radar solo se necessario.

---



Per usare WiFi Radar:

1. Andate su **Settings (Impostazioni)** e configurate tutti i parametri di WiFi Radar
1. Dal pannello di navigazione andate su **General (Generale)** > **WiFi Radar** e impostate la pianificazione per la registrazione dei dati.





2. Cliccate su **Start Data Collection**.
3. Dopo aver configurato tutti i parametri cliccate su **Submit**.

Home Site Survey Channel Statistics Advanced Troubleshooting Configure

**Settings**  
Configure all parameters of WiFi Radar

Sample Interval:  5 Second  10 Second  15 Second  20 Second

Start/Stop Data Collection

**Start Data Collection**

Start collecting data every

Sunday  Monday  Tuesday  Wednesday  Thursday  Friday  Saturday

From  To

Database Size

Database Size  MB  
(Please note that for example, 2.5743 s connected using a 5 seconds sample interval run for 1 hour will occupy approximately 1.30 MB of database)

Once Database size reaches maximum limit:  Overwrite Older Data  Stop Data Collection

Counters

- Channel Statistics
- Chann Statistics
- Rx CRS glitches
- Bad PCCP
- Bad FCS
- Packet Requested
- Packet Stored
- Packet Dropped
- Packet Retired
- Queue Utilization
- Queue Length Per Precedence
- Data Throughput
- Physical Rate
- RTS Fail
- Retry Drop
- PS Berry
- Alibid

**Submit**

Export Database

Download Database File **Save Database to File**

### 3.7.1 Verifica sito Wi-Fi

WiFi Site Survey (Verifica sito Wi-Fi) vi permette di scoprire le reti wireless presenti nei dintorni.



### 3.7.2 Statistiche canale wireless

Questa funzione mostra l'utilizzo corrente nel vostro ambiente di bande e canali tramite una distribuzione statistica.



### 3.7.3 Risoluzione dei problemi avanzata

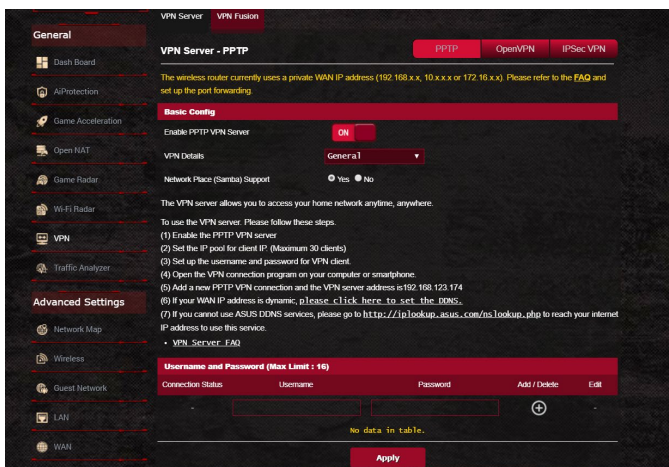
Questa funzione mostra una statistica degli errori delle reti Wi-Fi nel vostro ambiente.




## 3.8 VPN

Il servizio VPN (Virtual Private Network) instaura un canale di comunicazione sicura con un computer, o una rete, remoti usando l'infrastruttura pubblica della rete Internet.

**NOTA:** Prima di impostare una connessione VPN avrete bisogno di un indirizzo IP (o un nome del dominio) del server VPN.

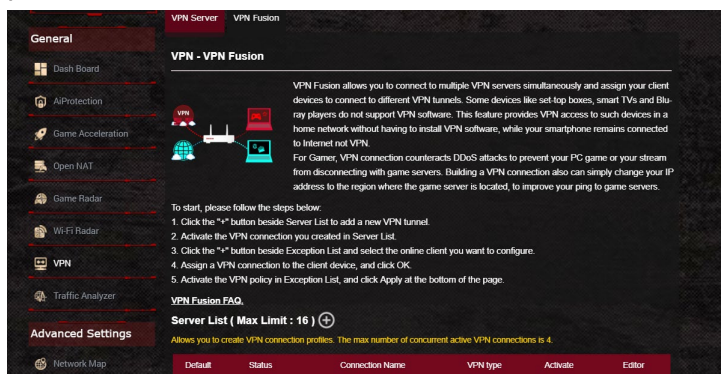


### Per configurare l'accesso ad un server VPN:

1. Dal pannello di navigazione andate su **General (Generale) > VPN**.
2. Alla voce **Enable PPTP VPN Server (Abilita server VPN PPTP)** selezionate **ON**.
3. Nell'elenco **VPN Details (Dettagli VPN)** selezionate **Advanced Settings (Impostazioni avanzate)** per configurare le impostazioni avanzate per la VPN come il supporto broadcast, l'autenticazione, la cifratura MPPE e il range di indirizzi IP per il client.
4. Alla voce **Network Place (Samba) Support (Supporto Risorse di rete (Samba))** selezionate **Yes (Sì)**.
5. Inserite nome utente e password necessari per accedere al server VPN. Cliccate su .
6. Cliccate su **Apply (Applica)**.

## 3.8.1 VPN Fusion

VPN Fusion vi permette di connettervi a server VPN multipli in simultanea e assegna i vostri dispositivi client a tunnel VPN differenti. Alcuni dispositivi come i decoder, le smart TV o i lettori Blu-ray non supportano il software VPN. Questa funzione fornisce accesso VPN a tali dispositivi connessi alla rete locale, senza bisogno di installare software VPN. Altri dispositivi, come il vostro smartphone, possono restare connessi ad Internet senza usare il tunnel VPN. Per gli utenti gamer la connessione VPN neutralizza gli attacchi DDoS per evitare che il PC si disconnetta dal server di gioco o lo streaming venga disconnesso. Una connessione VPN vi permette di ottenere un indirizzo IP nel paese in cui è presente il server di gioco, questo consentirà di migliorare il ping verso quel particolare server.



### Per iniziare seguite questi passaggi:

1. Cliccate sul pulsante “+” a fianco di **Elenco server** per aggiungere un nuovo tunnel VPN.
2. Attivate la connessione VPN creata in Elenco server.
3. Cliccate sul pulsante “+” a fianco di **Lista delle eccezioni** e selezionate il client online che volete configurare.
4. Assegnate una connessione VPN al dispositivo client e cliccate su **OK**.
5. Attivate le regole VPN in **Lista delle eccezioni** e cliccate su **Applica** al fondo della pagina.

### Server List ( Max Limit : 16 ) (+)

Allows you to create VPN connection profiles. The max number of concurrent active VPN connections is 4.

Default	Status	Connection Name	VPN type	Activate	Editor
<input checked="" type="checkbox"/>	Connected		Internet		
No data in table.					

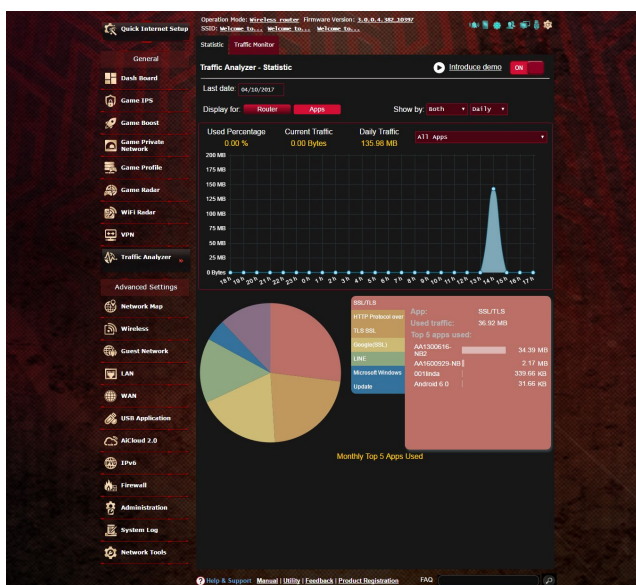
### Exception List ( Max Limit : 64 ) (+)

You can add VPN policies to the exception list, so that different client devices can connect to different VPN tunnels.

Client Name (MAC Address)	IP Address	Connection Name	Activate	Delete
No data in table.				
<input type="button" value="Apply"/>				

## 3.9 Traffic Analyzer

Traffic Analyzer presenta una panoramica di quanto sta succedendo nella vostra rete su base giornaliera, settimanale o mensile. Vi permette di visualizzare velocemente l'utilizzo di banda di ciascun utente e i dispositivi/app utilizzati, questo vi permette di ridurre i colli di bottiglia nella vostra connessione a Internet. Inoltre questo è un ottimo metodo per monitorare l'utilizzo di Internet e le attività degli utenti.



### Per configurare Traffic analyzer:

1. Dal pannello di navigazione andate su **General (Generale)** > **Traffic Analyzer**.
2. Nella pagina principale di **Traffic Analyzer** attivate le statistiche di traffic analyzer.
3. Selezionate la data per la quale volete visualizzare il grafico.
4. Nel campo **Display for** selezionate Router o App per visualizzare le informazioni del traffico.
5. Nel campo **Show by (Mostra per)** selezionate la modalità con la quale volete visualizzare le informazioni di traffico.

# 4 Configurare le Impostazioni avanzate

## 4.1 Usare la Mappa di rete

La Mappa di rete vi permette di configurare le impostazioni di sicurezza della vostra rete, gestire i diversi client e monitorare il vostro dispositivo USB.

The screenshot displays the web interface of an ASUSTeK router. At the top, it shows the operation mode as 'wireless\_router' and the firmware version as '3.0.0.4.384.80875'. The SSID is 'cocktailtoday' and the SSID mode is 'cocktailtoday\_5G'. The interface is divided into several sections:

- General:** Includes links for Quick Internet Setup, Dash Board, AiProtection, Game Acceleration, Open NAT, Game Radar, Wi-Fi Radar, VPN, and Traffic Analyzer.
- Advanced Settings:** Includes Network Map, Wireless, Guest Network, LAN, WAN, USB Application, AiCloud 2.0, Alexa & IFTTT, IPv6, Firewall, Administration, System Log, and Network Tools.
- System Status:** A table showing the status of 2.4GHz and 5GHz networks. The 2.4GHz network is named 'cocktailtoday' and is in a 'Personal' security mode with WPA2 encryption and AES. The 5GHz network is currently disabled.
- Network Map:** Shows the current network configuration, including Internet status (Connected), WAN IP (192.168.123.174), and DNS (GO). It also displays the security level as WPA2-Personal.
- Client and USB Status:** Shows 1 client connected to the wireless network and 0 AiMesh nodes. It also indicates that no USB 3.0 or USB 2.0 devices are connected.

At the bottom of the interface, there are links for Help & Support, Manual, Utility, and Product Registration, along with a FAQ link and a copyright notice for ASUSTeK Computer Inc. in 2019.

## 4.1.1 Configurare le impostazioni di protezione della rete wireless

Per proteggere la vostra rete wireless dagli accessi non autorizzati dovete configurare le sue impostazioni di protezione.

### Per configurare le impostazioni di protezione della rete wireless:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Network Map (Mappa di rete)**.
2. Dalla schermata **Network Map (Mappa di rete)**, nella sezione **System status (Stato del sistema)** potete visualizzare le impostazioni di protezione come la visibilità del SSID, il livello di sicurezza e la cifratura.

---

**NOTA:** Avete la possibilità di configurare diverse impostazioni di sicurezza per le due diverse bande di frequenza 2.4GHz e 5GHz.

---

### Impostazioni di protezione 2.4GHz

The screenshot shows the 'System Status' configuration screen for the 2.4GHz band. At the top, there are three tabs: '2.4GHz' (selected), '5GHz', and 'Status'. Below the tabs, the 'Network Name (SSID)' field contains the text 'cocktailtoday'. The 'Authentication Method' dropdown menu is set to 'WPA2-Personal'. The 'WPA Encryption' dropdown menu is set to 'AES'. The 'WPA-PSK key' field contains a series of asterisks. At the bottom, there is a red 'Apply' button.

### Impostazioni di protezione 5GHz

The screenshot shows the 'System Status' configuration screen for the 5GHz band. At the top, there are three tabs: '2.4GHz', '5GHz' (selected), and 'Status'. Below the tabs, the 'Network Name (SSID)' field contains the text 'cocktailtoday\_5G'. The 'Authentication Method' dropdown menu is set to 'WPA2-Personal'. The 'WPA Encryption' dropdown menu is set to 'AES'. The 'WPA-PSK key' field contains a series of asterisks. At the bottom, there is a red 'Apply' button.

3. Nel campo **Wireless name (Nome rete wireless) (SSID)** inserite un nome unico da assegnare alla vostra rete wireless.
4. Dall'elenco **Authentication Method (Metodo d'autenticazione)** selezionate la modalità di autenticazione per la vostra rete wireless.

Se selezionate WPA-Personal o WPA-2 Personal inserite la chiave WPA-PSK o la passkey di sicurezza.



**IMPORTANTE!** Gli standard IEEE 802.11n/ac impediscono l'uso di elevate velocità di trasferimento se utilizzate i metodi di cifratura WEP o WPA-TKIP. Se decidete di utilizzarli comunque la velocità della vostra rete sarà limitata allo standard IEEE 802.11g a 54 Mbps.

5 Quando avete finito cliccate su **Apply (Applica)**.

## 4.1.2 Gestione dei client di rete

The image shows two screenshots from the Mikrotik WinBox interface. The top screenshot is the 'General' settings page for the wireless network. It displays 'Internet status: Connected' with WAN IP 192.168.123.174 and DNS: GO. Under 'Wireless', it shows 'Security level: WPA2-Personal'. In the 'Clients' section, it indicates 'Clients: 1' and a 'View List' button is highlighted with a yellow box. The bottom screenshot shows the 'Client status' window, which is a table listing connected clients. The table has columns for Internet, Icon, Clients Name, Clients IP Address, Clients MAC Address, Interface, Tx Rate (Mbps), Rx Rate (Mbps), and Access time. Two clients are listed: 'android(Sony)' and 'HUAMEI\_Mate\_7'.

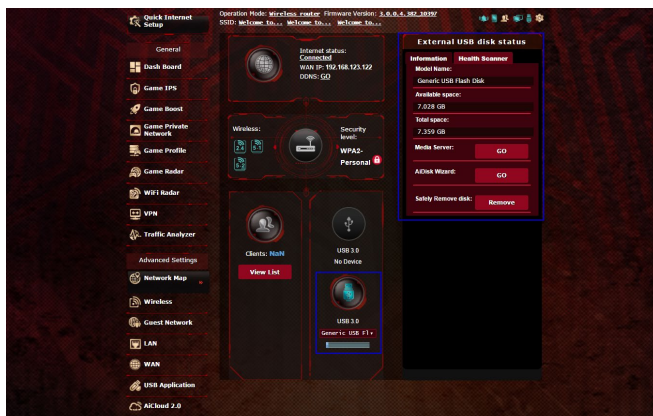
Internet	Icon	Clients Name	Clients IP Address	Clients MAC Address	Interface	Tx Rate (Mbps)	Rx Rate (Mbps)	Access time
Internet	Android	android(Sony)	192.168.1.116	DHCP A0:E4:53:FC:42:CA	eth1	433.3	40.5	02:50:55
Internet	Huawei	HUAMEI_Mate_7	192.168.1.201	DHCP E0:19:1D:EC:62:D7	eth1	150	13.5	02:31:02

**Per gestire i client della vostra rete:**

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Network Map (Mappa di rete)**.
2. Nella schermata **Network Map (Mappa di rete)** selezionate l'icona **Clients (Client)** per visualizzare le informazioni sui client della rete.
3. Cliccate su **View List** sotto all'icona **Clients** per visualizzare tutti i client.
4. Per bloccare l'accesso di un client alla vostra rete selezionate il client e cliccate sull'icona a forma di lucchetto aperto.

## 4.1.3 Controllo del vostro dispositivo USB

Il router wireless ASUS fornisce due porte USB per il collegamento di dispositivi USB, o stampanti USB, e permette di condividere i file, e la stampante, con tutti i client della vostra rete.



### NOTE:

- Per usare questa funzione è necessario inserire un dispositivo di archiviazione USB, come un hard disk USB o una memoria flash USB, in una delle porte USB 3.0/2.0 del pannello posteriore del vostro router wireless. Assicuratevi che il dispositivo di archiviazione USB sia formattato e partizionato correttamente. Fate riferimento all'elenco di dischi Plug-n-Share che trovate sul sito web: <http://event.asus.com/networks/disksupport>
- Le porte USB possono supportare contemporaneamente due dischi USB o una stampante USB e un disco USB.

**IMPORTANTE!** Dovete prima di tutto creare un account di condivisione, e i relativi permessi, per permettere agli altri client della rete di accedere al dispositivo USB tramite FTP, Gestione Server, Samba o AiCloud. Per maggiori dettagli fate riferimento alle sezioni 4.6 *Utilizzare le Applicazioni USB* e 4.7 *Utilizzo di AiCloud 2.0*.

## Per controllare il vostro dispositivo USB:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Network Map (Mappa di rete)**.
2. Nella schermata **Network Map (Mappa di rete)** selezionate l'icona **USB Disk Status (Stato disco USB)** per visualizzare le informazioni sul dispositivo USB.
3. Nel campo di configurazione guidata di AiDisk cliccate su **GO (Vai)** per configurare un server FTP dedicato alla condivisione di file tramite la rete Internet.


### NOTE:

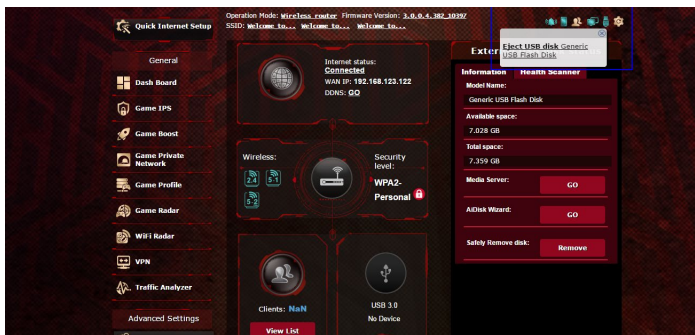
- Per maggiori dettagli fate riferimento alla sezione «4.6.2 Utilizzare il centro Gestione Server» di questo manuale.
- Il router wireless supporta la maggior parte dei dischi USB e delle memorie flash USB (fino a 4 TB di dimensione) e supporta accesso in lettura e in scrittura sui file system FAT16, FAT32, NTFS e HFS+.

## Rimozione sicura del disco USB

**IMPORTANTE:** Una rimozione non corretta del disco USB potrebbe causare perdite di dati.

### Per effettuare una rimozione sicura del disco USB:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Network Map (Mappa di rete)**.
2. Nell'angolo in alto a destra cliccate su  > **Eject USB disk (Espelli disco USB)**. Quando il disco USB è stato rimosso correttamente il campo USB Status (Stato USB) mostrerà il valore **Unmounted (Smontato)**.



## 4.1.4 ASUS AiMesh

### 4.1.4.1 Prerequisiti

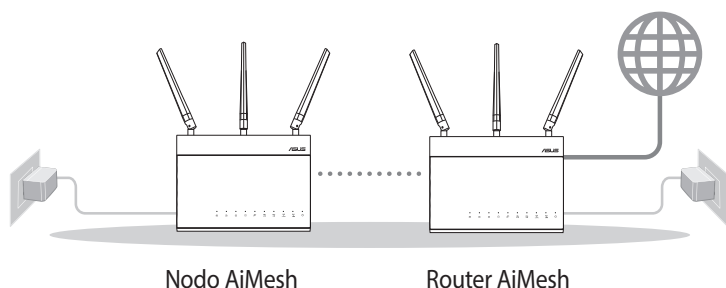
Configurazione di un sistema Wi-Fi AiMesh

1. Due (2) router ASUS (per conoscere i modelli che supportano AiMesh andate su <https://www.asus.com/AiMesh/>).
2. Uno di questi sarà il router AiMesh, l'altro sarà il nodo AiMesh.

---

**NOTA:** Se disponete di router AiMesh diversi raccomandiamo di utilizzare il router più performante come router AiMesh e gli altri come nodi AiMesh.

---



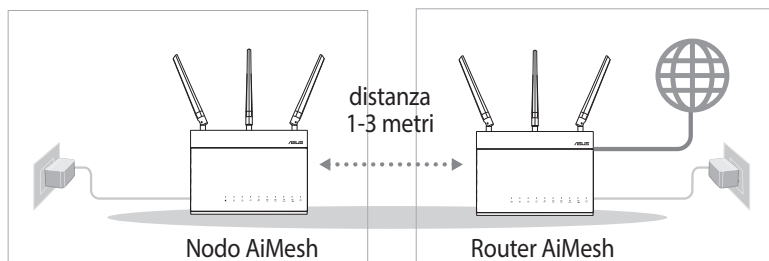
### 4.1.4.2 Configurazione di AiMesh

#### Preparazione

Posizionate il vostro router AiMesh e il nodo ad una distanza compresa tra 1 e 3 metri, l'uno dall'altro, durante il processo di configurazione.

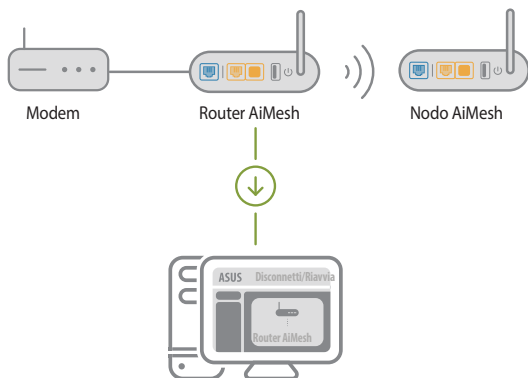
#### Nodo AiMesh

Il dispositivo è inizializzato con le impostazioni predefinite di fabbrica. Accendete il dispositivo e tenetelo in attesa della configurazione AiMesh.



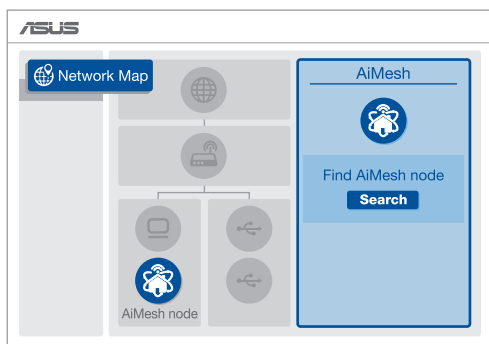
## Router AiMesh

- 1) Fate riferimento alla **Guida rapida** dell'altro router per collegare il vostro router AiMesh a PC e modem, quindi eseguite l'accesso all'interfaccia web (GUI).



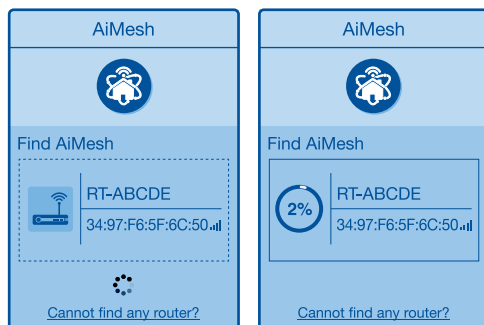
- 2) Andate alla pagina **Mappa di rete**, cliccate sull'icona AiMesh e poi su **Cerca** per cercare il nodo AiMesh.

**NOTA:** Se non trovate l'icona AiMesh cliccate su **Versione del firmware** e aggiornate il firmware.

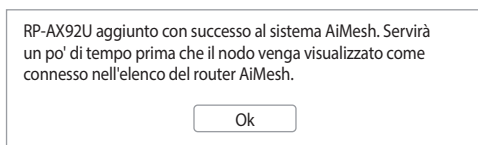


- 3) Cliccate su **Cerca**, il sistema cercherà automaticamente il vostro nodo AiMesh. Quando il nodo AiMesh verrà rilevato e visualizzato su questa pagina cliccate su di esso per aggiungerlo al sistema AiMesh.

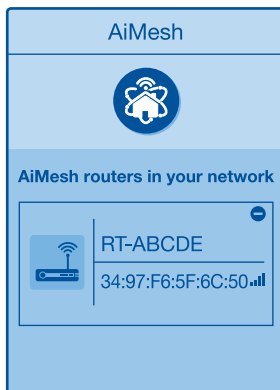
**NOTA:** Se non riuscite a trovare alcun nodo AiMesh andate alla sezione «RISOLUZIONE DEI PROBLEMI».



- 4) A sincronizzazione completata verrà visualizzato un messaggio.



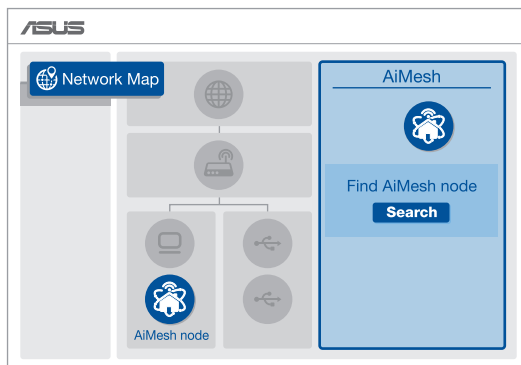
- 5) Congratulazioni! Quando un nodo AiMesh viene aggiunto correttamente alla rete AiMesh verrà visualizzato un messaggio di questo tipo.



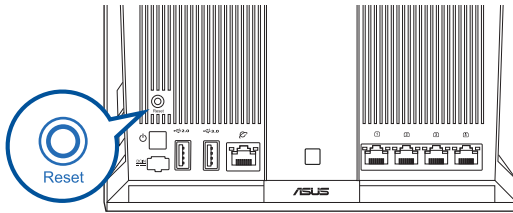
### 4.1.4.3 Risoluzione dei problemi

Se il vostro router AiMesh non trova alcun nodo AiMesh nelle vicinanze, o se la sincronizzazione fallisce, consultate questa sezione e riprovate.

- 1) Spostate il vostro nodo AiMesh più vicino al router AiMesh. Assicuratevi che i dispositivi siano ad una distanza compresa tra 1 e 3 metri.
- 2) Assicuratevi che il vostro nodo AiMesh sia acceso.
- 3) Se fosse necessario aggiornate il nodo AiMesh ad un firmware che supporti la funzione AiMesh.
  - i. Scaricate il firmware compatibile AiMesh da: <https://www.asus.com/AiMesh/>
  - ii. Accendete il vostro nodo AiMesh e collegatelo al vostro PC usando un cavo di rete.
  - iii. Avviate l'interfaccia web (GUI). Si aprirà automaticamente ASUS Setup Wizard. In caso contrario aprite la pagina <http://router.asus.com>
  - iv. Andate su **Amministrazione > Aggiornamento del firmware**. Cliccate su **Selezione file** e caricate il firmware compatibile con AiMesh.
  - v. Dopo aver aggiornato il firmware andate sulla pagina **Mappa di rete** e verificate che sia presente l'icona AiMesh.



- vi. Premete il pulsante di reset sul nodo AiMesh per almeno 5 secondi. Quando il LED di alimentazione lampeggia lentamente rilasciate il pulsante di reset.



#### 4.1.4.4 Riposizionamento

##### Per ottenere le prestazioni migliori:

Posizionate il router AiMesh e il nodo nella miglior posizione possibile.

---

##### NOTE:

- Per minimizzare le interferenze tenete i router lontani da dispositivi come telefoni cordless, dispositivi Bluetooth e forni a microonde.
  - Vi raccomandiamo di installare i router in un ambiente aperto e spazioso.
- 



#### 4.1.4.5 Domande e risposte frequenti (FAQ)

##### D1: Il router AiMesh supporta la modalità Access Point?

**R:** Sì. Potete scegliere di configurare il router AiMesh nelle modalità router o access point. Entrate nell'interfaccia web (GUI) (<http://router.asus.com>) e andate su **Amministrazione** > **Modalità operativa**.



## D2: Posso configurare una connessione cablata tra i router AiMesh (Ethernet backhaul)?

**R:** Sì. Il sistema AiMesh supporta entrambe le connessioni cablate e senza fili tra il router AiMesh e il nodo, per ottimizzare il throughput e la stabilità. AiMesh analizza la qualità del segnale senza fili per ciascuna frequenza e banda disponibile, in seguito AiMesh determina automaticamente quale tra la connessione cablata e la connessione senza fili è più adeguata per implementare il collegamento di dorsale tra i router.

- 1) Inizialmente seguite i passaggi di configurazione per stabilire la connessione senza fili tra il router AiMesh e il nodo.
- 2) Posizionate il nodo nella posizione ideale per ottenere copertura massima. Collegate un cavo dalla porta LAN del router AiMesh alla porta WAN del nodo AiMesh.

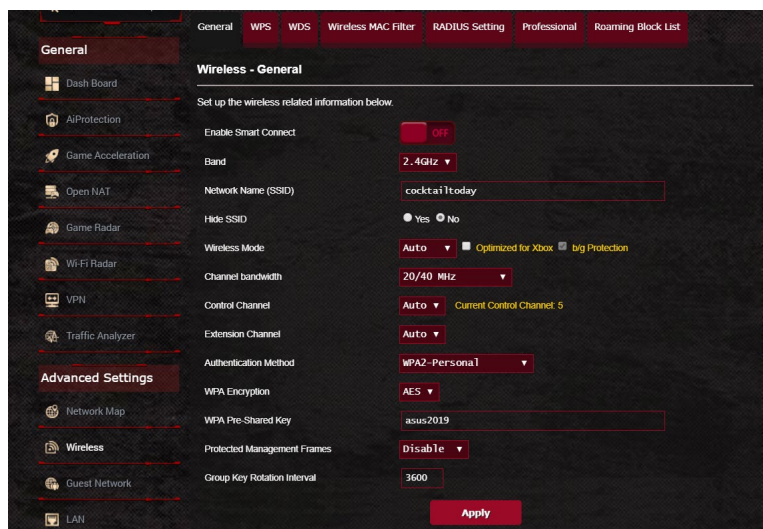


- 3) Il sistema AiMesh selezionerà automaticamente il percorso migliore per la trasmissione dei dati.

## 4.2 Wireless

### 4.2.1 Generale

La scheda **Generale** vi permette di configurare le opzioni di base della vostra connessione wireless.



### Per configurare le impostazioni base della connessione wireless:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate)** > **Wireless** e selezionate la scheda **General (Generale)**.
2. Selezionate 2.4GHz o 5GHz per scegliere la banda di frequenza per la vostra rete wireless.
3. Se volete usare la funzione Smart Connect spostate il cursore di **Enable Smart Connect** su **ON**. Questa funzione connette automaticamente i clienti della vostra rete alla banda più appropriata (2.4GHz o 5GHz) per una velocità ottimale.

4. Selezionate un nome univoco, al massimo di 32 caratteri, per il vostro SSID (Service Set Identifier) che identifica la vostra rete wireless. I dispositivi WiFi possono rilevare e connettersi alle reti wireless tramite il SSID. La lista degli SSID trovati dai dispositivi è aggiornata dopo che il SSID modificato è stato salvato nelle impostazioni.

---

**NOTA:** Potete assegnare SSID unici per entrambe le bande di frequenza 2.4GHz e 5GHz.

---

5. Nel campo **Hide SSID (Nascondi SSID)** selezionate **Yes (Sì)** per impedire agli altri dispositivi wireless di vedere il vostro SSID. Quando questa opzione è abilitata avrete bisogno di inserire il SSID sul vostro dispositivo wireless manualmente.
6. Selezionate una di queste **Modalità wireless** per determinare la tipologia dei dispositivi che possono connettersi al vostro router wireless:
  - **Auto:** Selezionate **Auto (Automatico)** per permettere la connessione ai dispositivi 802.11ac, 802.11n, 802.11g e 802.11b.
  - **Solo N:** Selezionate **N only (Solo N)** per massimizzare le prestazioni wireless N. Questa impostazione impedisce ai dispositivi 802.11g e 802.11b di connettersi al router wireless.
  - **Legacy:** Selezionate **Legacy** per permettere la connessione ai dispositivi 802.11b/g/n. I dispositivi che supportano 802.11n, in ogni caso, lavoreranno alla velocità massima di 54 Mbps.
7. Selezionate il canale operativo/di controllo per il vostro router wireless. Selezionate **Auto (Automatico)** per permettere al router di scegliere automaticamente il canale con la minore interferenza possibile.
8. Selezionate la larghezza del canale per favorire maggiori velocità di trasferimento.
9. Selezionate il metodo di autenticazione.
10. Quando avete finito cliccate su **Apply (Applica)**.

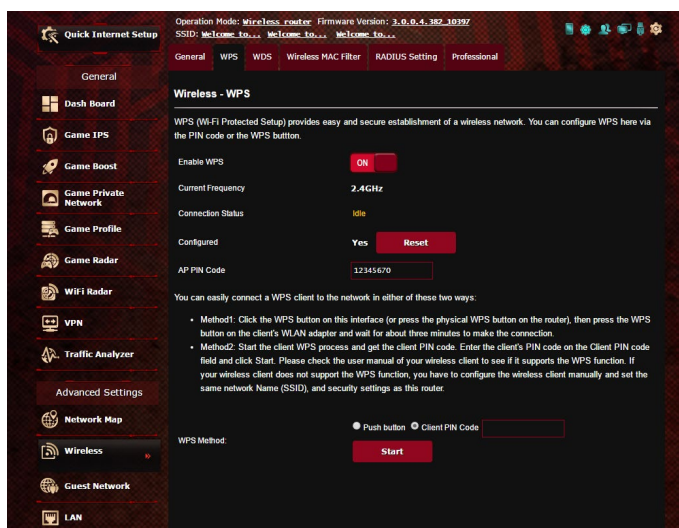
## 4.2.2 WPS

WPS (Wi-Fi Protected Setup) è uno standard di sicurezza wireless che vi permette di collegare facilmente i vostri dispositivi alla rete wireless. Potete configurare WPS tramite un codice PIN o con il pulsante WPS.

---

**NOTA:** Assicuratevi che i dispositivi supportino WPS.

---



**Per abilitare il WPS sulla vostra rete wireless:**

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Wireless** e selezionate la scheda **WPS**.
2. Nel campo **Enable WPS (Abilita WPS)** spostate il cursore su **ON**.
3. WPS utilizza la frequenza predefinita 2.4 Ghz. Se volete cambiare la frequenza scegliendo 5 Ghz spostate il cursore su **OFF**, cliccate su **Switch Frequency (Cambia frequenza)** e spostate nuovamente il cursore su **ON**.

---

**NOTA:** WPS supporta autenticazione tramite Open System, WPA-Personal e WPA2-Personal. WPS non supporta una rete wireless che usa una metodi di cifratura a chiave condivisa, WPA-Enterprise, WPA2-Enterprise e RADIUS.

---

4. Nel campo **WPS Method (Modalità WPS)** selezionate **Push Button (Premi Pulsante)** o **Client PIN code (Codice PIN client)**. Se selezionate **Push Button (Premi Pulsante)** andate al passaggio 5. Se selezionate **Client PIN code (Codice PIN client)** andate al passaggio 6.
5. Per impostare il WPS usando il pulsante WPS del router procedete nel modo seguente:
  - a. Cliccate su **Start (Avvia)** o premete il pulsante WPS che trovate nella parte posteriore del router wireless.
  - b. Premete il pulsante WPS sul vostro dispositivo wireless. Di solito questo pulsante è identificato dal logo WPS.

---

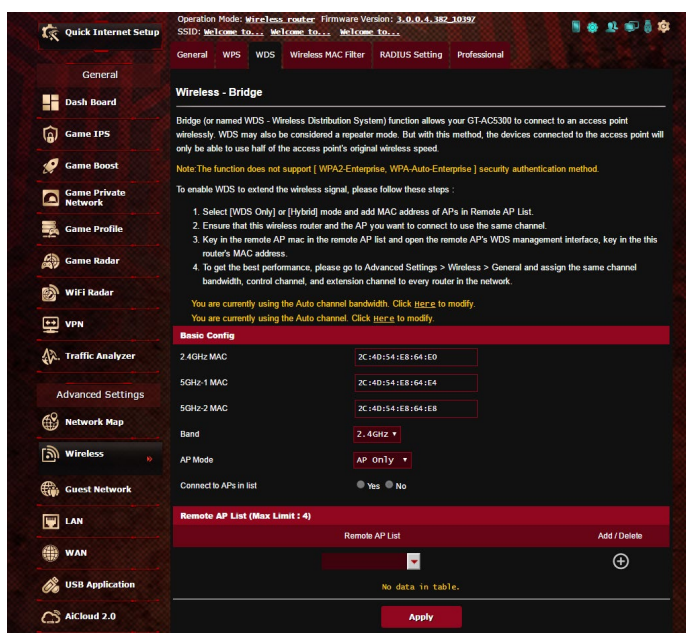
**NOTA:** Controllate il vostro dispositivo wireless, o il relativo manuale utente, per verificare la posizione del pulsante WPS.

---

- c. Il router wireless cercherà i dispositivi WPS disponibili. Se il router wireless non trova nessun dispositivo WPS entrerà in standby.
6. Per impostare il WPS usando il codice PIN client procedete nel modo seguente:
  - a. Individuate il codice PIN WPS sul manuale utente del vostro dispositivo wireless o sul dispositivo stesso.
  - b. Inserite il codice PIN client nella casella di testo relativa.
  - c. Cliccate su **Start (Avvia)** per dire al router di entrare in modalità rilevamento WPS. Gli indicatori LED del router lampeggiano velocemente per tre volte fino a quando la configurazione WPS è completata.

## 4.2.3 Bridge

La modalità Bridge, o WDS (Wireless Distribution System), permette al vostro router wireless di connettersi ad un altro access point wireless in maniera più o meno esclusiva impedendo ad altri dispositivi wireless, o stazioni, di connettersi al vostro router wireless ASUS. In alternativa, il router wireless, si può comportare come repeater wireless. In questo caso il router wireless ASUS comunicherà con un altro access point wireless e con altri dispositivi wireless (ibrido).



Per configurare il bridge wireless:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Wireless** e selezionate la scheda **WDS**.
2. Selezionate la banda di frequenza per il bridge wireless.

3. Nel campo **AP Mode (Modalità AP)** selezionate una delle seguenti opzioni:
  - **AP Only (Solo AP):** Disabilita la funzionalità Bridge Wireless.
  - **WDS Only (Solo WDS):** Abilita la funzionalità Bridge Wireless ma impedisce agli altri dispositivi/stazioni di connettersi al router.
  - **IBRIDO:** Abilita la funzionalità Bridge Wireless e permette ad altri dispositivi/stazioni wireless di connettersi al router.

---

**NOTA:** Nella modalità **IBRIDO** i dispositivi wireless connessi al router wireless ASUS riceveranno solamente metà della banda disponibile dell'Access Point.

---


4. Nel campo **Connect to APs in list (Connetti ad AP nell'elenco)** selezionate **Yes (Sì)** se volete connettervi ad un Access Point presente nell'elenco degli AP remoti.
5. Come impostazione standard il canale operativo/di controllo viene scelto in automatico per permettere al router di scegliere il canale con la minore interferenza possibile.

Potete modificare il **Control Channel (Canale di controllo)** in **Advanced Settings (Impostazioni avanzate) > Wireless > General (Generale)**.

---

**NOTA:** La disponibilità dei canali wireless varia in base al Paese o alla regione.

---

6. In **Elenco AP remoti** inserite un indirizzo MAC e cliccate sul pulsante **Add (Aggiungi)**  per inserire l'indirizzo MAC di altri Access Point disponibili.

---

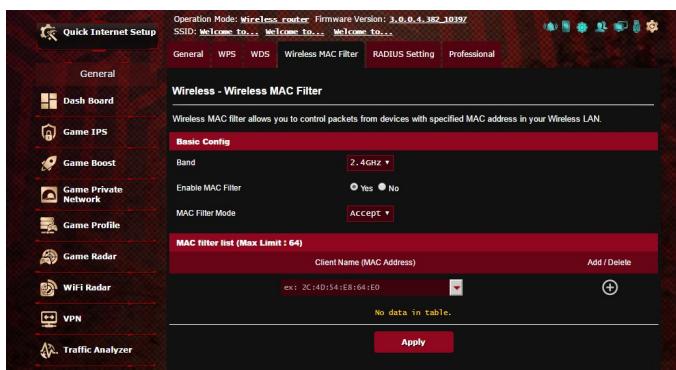
**NOTA:** Ogni Access Point aggiunto alla lista deve essere configurato sullo stesso canale di controllo del router wireless ASUS.

---

7. Cliccate su **Apply (Applica)**.

## 4.2.4 Filtro MAC wireless

Il Filtro MAC wireless fornisce controllo sui pacchetti trasmessi verso uno specifico indirizzo MAC (Media Access Control) presente nella vostra rete wireless.



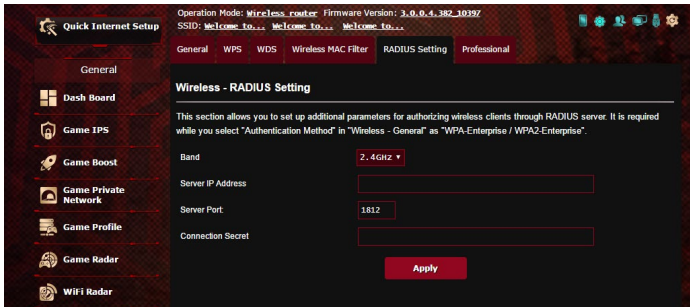
### Per impostare il Filtro MAC wireless:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate)** > **Wireless** e selezionate la scheda **Wireless MAC Filter (Filtro MAC Wireless)**.
2. Alla voce **Enable MAC Filter (Abilita filtro MAC)** selezionate **Yes (Sì)**.
3. Nel menu **MAC Filter Mode (Modalità filtro MAC)** selezionate **Accept (Accetta)** o **Reject (Rifuta)**.
  - Selezionate **Accept (Accetta)** per permettere agli indirizzi MAC nell'elenco di accedere alla rete wireless.
  - Selezionate **Reject (Rifuta)** per impedire agli indirizzi MAC nell'elenco di accedere alla rete wireless.
4. In **Elenco filtro MAC** cliccate sul pulsante **Add (Aggiungi)**  e inserite l'indirizzo MAC del dispositivo wireless.
5. Cliccate su **Apply (Applica)**.



## 4.2.5 Impostazioni RADIUS

Il servizio RADIUS (Remote Authentication Dial In User Service) fornisce un ulteriore livello di sicurezza nel caso si siano selezionate le modalità di autenticazione WPA-Enterprise, WPA2-Enterprise o Radius 802.1x.



### Per configurare le impostazioni wireless RADIUS:

1. Assicuratevi che la modalità di autenticazione wireless del router sia impostata su WPA-Enterprise o WPA2-Enterprise.

---

**NOTA:** Fate riferimento alla sezione «4.2.1 Generale» per la configurazione della modalità di autenticazione del vostro router wireless.

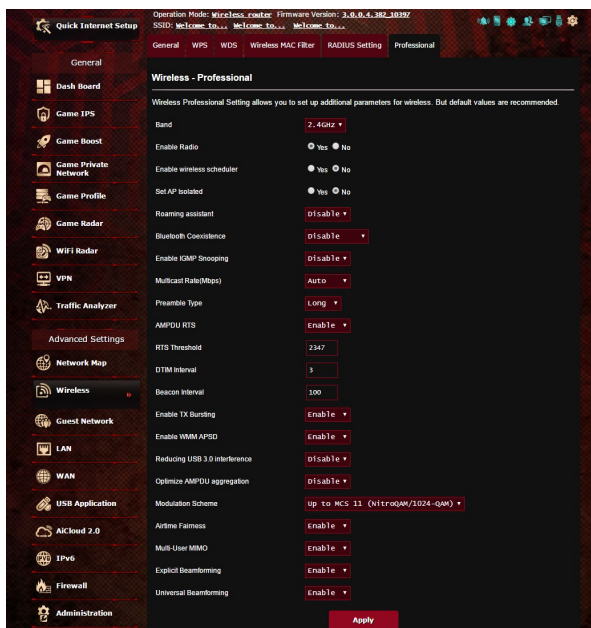
---

2. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Wireless** e selezionate la scheda **RADIUS Setting (Impostazioni RADIUS)**.
3. Selezionate la frequenza.
4. Nel campo **Server IP Address (Indirizzo IP server)** inserite l'indirizzo IP del server RADIUS.
5. Nel campo **Server Port (Porta server)** inserite la porta del server.
6. Nel campo **Connection Secret** inserite la password per accedere al server RADIUS.
7. Cliccate su **Apply (Applica)**.

## 4.2.6 Professionale

La schermata Professionale fornisce opzioni di configurazione avanzata.

**NOTA:** Vi raccomandiamo di utilizzare i valori predefiniti per questa pagina.



Nella schermata **Professional (Professionale)** potete configurare le seguenti opzioni:

- **Frequenza:** Selezionate la banda di frequenza.
- **Enable Radio (Abilita WiFi):** Selezionate **Yes (Sì)** per abilitare la rete wireless. Selezionate **No** per disabilitarla.
- **Date to Enable Radio (weekdays) (Giorni in cui abilitare WiFi (lun-ven)):** Potete scegliere in quali giorni della settimana abilitare la rete wireless.
- **Time of Day to Enable Radio (Ora del giorno in cui abilitare WiFi):** Potete scegliere un intervallo di tempo in cui abilitare la rete wireless nei giorni selezionati della settimana.
- **Date to Enable Radio (weekend) (Giorni in cui abilitare WiFi (sab-dom)):** Potete scegliere in quali giorni del weekend abilitare la rete wireless.

- **Time of Day to Enable Radio (Ora del giorno in cui abilitare WiFi):** Potete scegliere un intervallo di tempo in cui abilitare la rete wireless nei giorni selezionati del weekend.
- **Set AP isolated (Imposta Isolamento AP):** L'opzione **Imposta Isolamento AP** impedisce ai dispositivi wireless della vostra rete di comunicare tra di loro. Questa caratteristica è utile se molti dispositivi diversi accedono e lasciano la vostra rete di frequente. Selezionate **Yes (Sì)** per abilitare questa funzione, **No** per disabilitarla.
- **Roaming Assistant (Assistente roaming):** Nelle configurazioni di rete che prevedono diversi access point, o repeater wireless, i client wireless a volte non riescono a connettersi automaticamente agli AP disponibili perché sono ancora connessi al router principale. Abilitate questa impostazione in modo che il client si possa disconnettere dal router principale, nel caso in cui il segnale sia più basso di una soglia specifica, per connettersi ad un segnale più potente.
- **Enable IGMP Snooping (Abilita IGMP Snooping):** Abilitando questa funzione abilitate l'IGMP (Internet Group Management Protocol) per ottimizzare il traffico multicast.
- **Multicast rate (Mbps) (Velocità multicast (Mbps)):** Selezionate la velocità del multicast o **Disable (Disabilita)** se volete impedire le trasmissioni singole simultanee.
- **Preamble Type (Tipo di preambolo):** Definisce quanto tempo deve spendere il router per il controllo CRC (Cyclic Redundancy Check). CRC è un metodo che si occupa di rilevare gli errori durante la trasmissione di dati. Selezionate **Short (Corto)** per una rete wireless molto frequentata con elevato traffico di rete. Selezionate **Long (Lungo)** se la vostra rete wireless è frequentata da dispositivi wireless datati.
- **AMPDU RTS:** Questa funzione permette di unire un gruppo di pacchetti prima che questi vengano trasmessi e usare RTS per ogni AMPDU nel caso delle comunicazioni tra dispositivi 802.11g e 802.11b.
- **RTS Threshold (Soglia RTS):** Un valore più basso di Soglia RTS (Request to Send) migliorerà la comunicazione wireless in una rete affollata e con elevato traffico di rete.
- **Intervallo DTIM:** L'intervallo DTIM (Delivery Traffic Indication Message) è l'intervallo di tempo che passa prima dell'invio di un segnale di risveglio, verso un dispositivo wireless che

è in sospensione, per indicare che un pacchetto di dati sta aspettando per la consegna. Il valore standard è di 3 millisecondi.

- **Beacon Interval (Intervallo Beacon):** L'intervallo Beacon (Beacon Interval) è il periodo di tempo che passa tra un DTIM e il successivo. Il valore predefinito è 100 millisecondi. Abbassate il valore dell'intervallo Beacon nel caso di rete wireless instabile o per dispositivi in roaming.
- **Enable TX Bursting (Abilita TX Burst):** Migliora la velocità di trasferimento tra il router wireless e i dispositivi 802.11g.
- **Enable WMM APSD (Abilita APSD WMM):** Abilitate la funzione APSD WMM (Wi-Fi Multimedia Automatic Power Save Delivery) per migliorare la gestione dell'energia, e della banda, nei confronti di dispositivi wireless compatibili. Selezionate **Disable (Disabilita)** per disattivare APSD WMM.
- **Riduzione delle interferenze USB 3.0:** Questa funzione garantisce le migliori prestazioni wireless per la banda 2.4 GHz. Disabilitando questa funzione aumenterete la velocità di trasferimento della porta USB 3.0 ma influenzerete la banda 2.4 GHz.
- **Ottimizza aggregazione A-MPDU:** Ottimizza il numero massimo di MPDU in un AMPDU ed evita che i pacchetti vengano persi o corrotti durante la trasmissione in canali wireless con errori
- **Ottimizza rimozione ACK:** Ottimizza il numero di ACK eliminabili contemporaneamente.
- **Turbo QAM:** Questa funzione fornisce supporto a 256-QAM (MCS 8/9) per la banda 2.4 GHz per avere un range e una trasmissione migliori su quella frequenza.
- **Airtime Fairness:** In questo modo la velocità della rete non è determinata dal traffico più lento. Grazie all'allocazione temporale uniforme per ciascun client ogni trasmissione è in grado di procedere alla sua velocità massima potenziale.
- **Explicit Beamforming (Beamforming esplicito):** L'adattatore WLAN del client e il router supportano entrambi la tecnologia beamforming. Questa tecnologia permette ai dispositivi di comunicare tra di loro informazioni riguardanti la stima dei parametri del canale per aumentare le velocità di download e upload.

- **Beamforming universale:** Per gli adattatori wireless datati, che non supportano il beamforming, il router stima automaticamente le migliori impostazioni per aumentare le velocità di download e upload.

## 4.3 Creare una Rete ospiti

Una **Guest Network (Rete ospiti)** fornisce ai visitatori temporanei una connessione ad Internet, tramite una rete diversa (SSID differente), senza fornire accesso alla vostra rete privata.

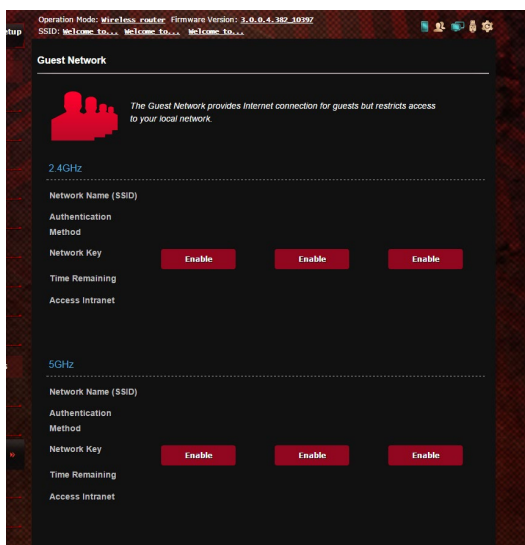
---

**NOTA:** GT-AC2900 può gestire fino a sei SSID (tre SSID a 2.4GHz e tre SSID a 5GHz).

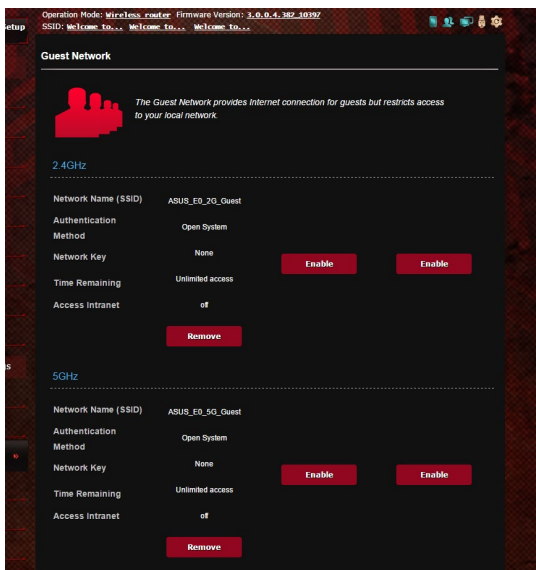
---

### Per creare una Rete ospiti:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Guest Network (Rete ospiti)**.
2. Nella schermata Rete ospiti selezionate quale banda di frequenza desiderate usare per la rete ospiti che intendete creare: 2.4Ghz o 5Ghz.
3. Cliccate su **Enable (Abilita)**.



4. Per modificare le impostazioni di una rete ospiti cliccate sulla rete che volete modificare. Cliccate su **Remove (Rimuovi)** per eliminare la rete ospiti corrispondente.
5. Scegliete un nome per la vostra rete temporanea indicandolo nel campo **Network Name (Nome della rete) (SSID)**.



6. Selezionate un metodo di autenticazione.
7. Se avete scelto l'autenticazione WPA selezionate la cifratura WPA.
8. Specificate l'**Access time (Durata Accesso)** o scegliete **Limitless (Illimitato)**.
9. Alla voce **Access Intranet (Accesso Intranet)** selezionate **Disable (Disabilita)** o **Enable (Abilita)**.
10. Quando avete finito cliccate su **Apply (Applica)**.

## 4.4 LAN

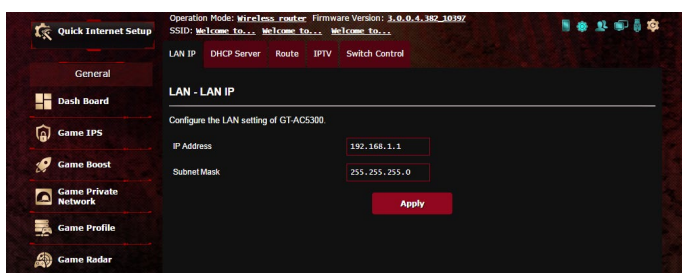
### 4.4.1 LAN IP

La schermata LAN IP permette di modificare le impostazioni LAN del router wireless.

---

**NOTA:** Qualsiasi cambiamento dell'IP LAN del vostro router avrà effetti automaticamente anche sulle impostazioni del server DHCP.

---



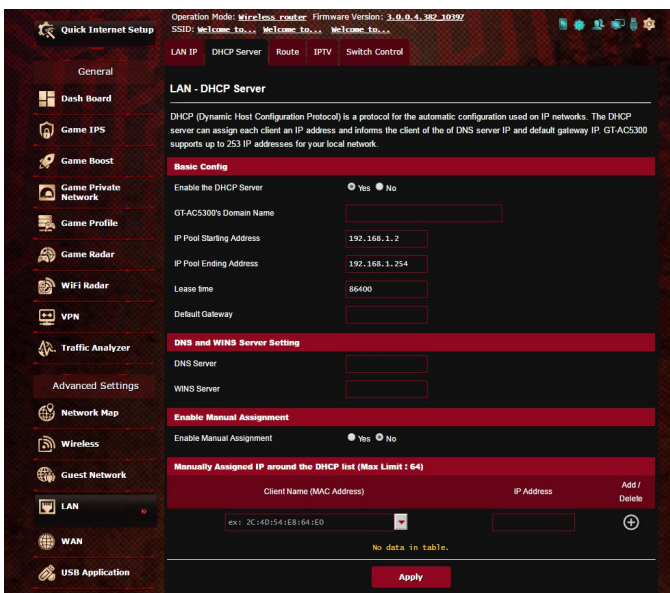
**Per modificare le impostazioni LAN del router wireless:**

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate)** > **LAN** e selezionate la scheda **LAN IP (IP LAN)**.
2. Potete modificare i campi **IP Address** e **Subnet Mask**.
3. Quando avete finito cliccate su **Apply (Applica)**.



## 4.4.2 Server DHCP

Il vostro router wireless usa il protocollo DHCP per assegnare indirizzi IP nella vostra rete automaticamente. Potete specificare l'intervallo di indirizzi IP e il tempo di rilascio per i client della vostra rete.



**Per configurare il server DHCP:**

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > LAN** e selezionate la scheda **DHCP Server (Server DHCP)**.
2. Alla voce **Enable the DHCP Server (Abilita il server DHCP)** selezionate **Yes (Sì)**.
3. Nel campo **Domain Name (Nome del Dominio)** inserite un nome di dominio per il router wireless.
4. Nel campo **IP Pool Starting Address (Indirizzo IP iniziale)** inserite l'indirizzo IP iniziale dell'intervallo desiderato.

5. Nel campo **IP Pool Ending Address (Indirizzo IP finale)** inserite l'indirizzo IP finale dell'intervallo desiderato.
6. Nel campo **Lease Time (Tempo di rilascio)** specificate, in termini di secondi, la durata dell'assegnazione di un indirizzo IP. Una volta raggiunto il tempo di rilascio il server DHCP assegnerà al client un nuovo indirizzo IP.

---

**NOTE:**

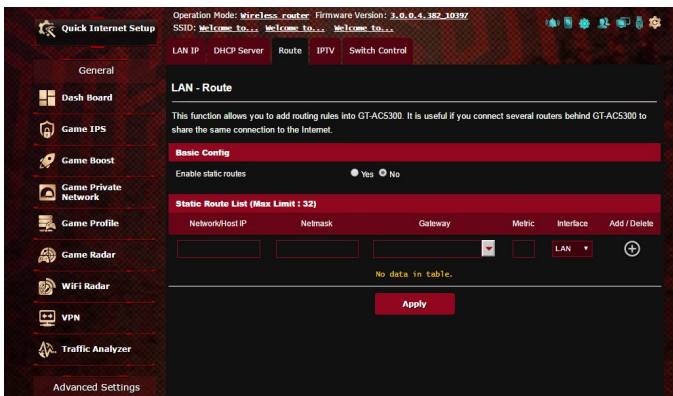
- Raccomandiamo di utilizzare un indirizzo IP del formato 192.168.1.xxx (con xxx che può variare da 2 a 254) quando dovete scegliere un intervallo di indirizzi IP.
  - L'indirizzo IP iniziale non deve essere superiore all'indirizzo IP finale.
- 

7. Nella sezione **DNS and WINS Server Setting (Impostazione server DNS e WINS)** inserite gli indirizzi IP dei server DNS e WINS se necessario.
8. Il vostro router wireless è anche in grado di assegnare manualmente gli indirizzi IP ai dispositivi della rete. Alla voce **Enable Manual Assignment (Abilita assegnazione manuale)** selezionate **Yes (Sì)** per assegnare un indirizzo IP ad un indirizzo MAC specifico sulla rete. Potete specificare fino a 32 indirizzi MAC nell'elenco DHCP di assegnazione manuale degli indirizzi IP.



## 4.4.3 Rotte

Se la vostra rete usa uno o più router wireless potete configurare una tabella di routing in modo da condividere la stessa connessione ad Internet.

**NOTA:** Vi raccomandiamo di non modificare la tabella di routing predefinita a meno che non abbiate una conoscenza approfondita delle tabelle di routing.

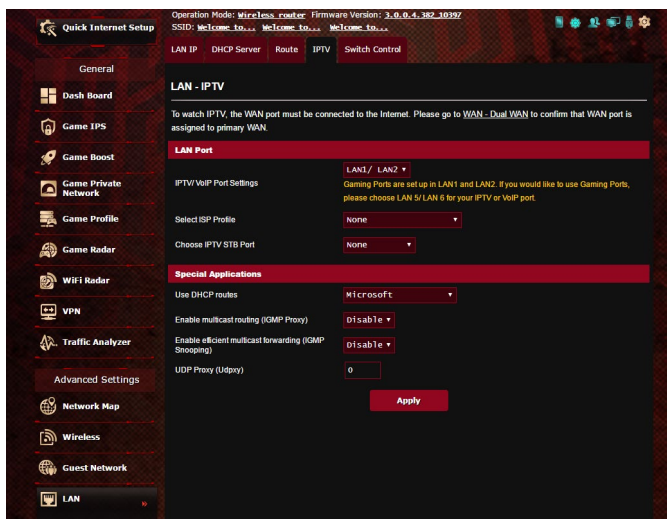


**Per configurare la tabella di routing:**

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate)** > **LAN** e selezionate la scheda **Route (Rotte)**.
2. Selezionate **Yes (Sì)** alla voce **Enable static routes (Abilita routing statico)**.
3. Nell'elenco **Static Route List (Rotte Statiche)** inserite le informazioni di rete degli altri access point o nodi. Cliccate sul pulsante **Add (Aggiungi)**  o **Delete (Elimina)**  per aggiungere o rimuovere un dispositivo dall'elenco.
4. Cliccate su **Apply (Applica)**.

## 4.4.4 IPTV

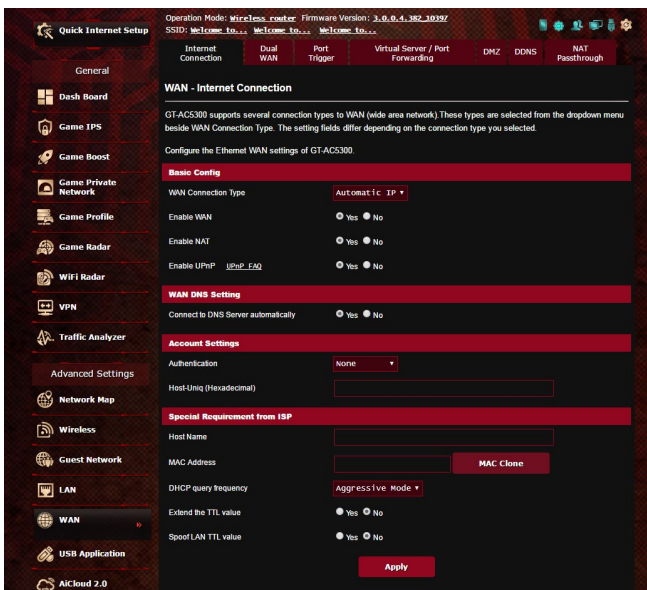
Il router wireless supporta la connessione a servizi IPTV tramite ISP o LAN. La scheda IPTV vi permette di configurare le varie impostazioni per i servizi IPTV, VoIP, multicasting e UDP. Contattate il vostro ISP per maggiori informazioni sui servizi disponibili con la vostra fornitura.



## 4.5 WAN

### 4.5.1 Connessione ad Internet

La schermata **Connessione ad Internet** vi permette di configurare le varie impostazioni per la connessione WAN.



**Per configurare le impostazioni della connessione WAN:**

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > WAN** e selezionate la scheda **Internet Connection (Connessione ad Internet)**.
2. Configurate le seguenti impostazioni. Quando avete finito cliccate su **Apply (Applica)**.
  - **Tipo di connessione WAN:** Scegliete il protocollo di connessione ad Internet in base alle indicazioni del vostro ISP. Le scelte sono le seguenti: **Automatic IP (IP automatico)**, **PPPoE**, **PPTP**, **L2TP** o **Static IP (IP statico)**. Contattate il vostro ISP nel caso in cui il vostro router non riuscisse ad ottenere un indirizzo IP valido o se non siete sicuri del tipo di connessione WAN.

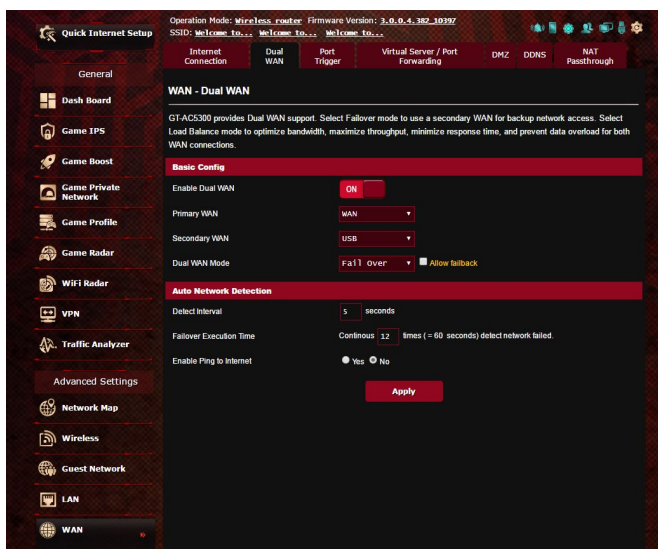
- **Abilita WAN:** Selezionate **Yes (Sì)** per permettere al router di accedere ad Internet. Selezionate **No** per impedirlo.
- **Abilita NAT:** Il servizio NAT (Network Address Translation) prevede che un unico indirizzo IP pubblico (WAN) possa essere usato per condividere l'accesso ad Internet a diversi client presenti nella rete locale (LAN) assegnando a ciascuno di essi un indirizzo IP privato. L'indirizzo IP privato di ogni client della rete locale è salvato in una tabella di NAT ed è usato per instradare i pacchetti di dati in entrata.
- **Abilita UPnP:** Il protocollo UPnP (Universal Plug and Play) permette a diversi dispositivi (come router, televisioni, sistemi stereo, console di gioco e telefoni cellulari) di essere controllati all'interno di una rete IP con, o senza, il bisogno di un controller centrale come potrebbe essere un gateway. UPnP connette PC di vario tipo fornendo funzionalità di rete per la configurazione remota e il trasferimento dati. Usando UPnP un nuovo dispositivo di rete viene rilevato automaticamente. Una volta collegati in rete i dispositivi possono essere configurati da remoto per supportare applicazioni P2P (peer-to-peer), gioco online, video conferenze e server proxy o web. A differenza del Port Forwarding, il quale richiede la configurazione manuale delle porte, UPnP configura automaticamente il router ad accettare le connessioni in ingresso e indirizzare le richieste ad un PC specifico sulla rete locale.
- **Connetti automaticamente al Server DNS:** Ordina al router di ottenere automaticamente dall'ISP l'indirizzo IP del Server DNS. Un Server DNS è un'entità presente nella rete Internet che si occupa di tradurre gli indirizzi Internet nei corrispondenti indirizzi IP.
- **Autenticazione:** Questo campo potrebbe essere richiesto da alcuni ISP. Verificate con il vostro ISP e compilate questo campo se necessario.

- **Nome Host:** Questo campo vi permette di inserire un Nome Host per il vostro router. Di solito è un requisito speciale richiesto da alcuni ISP. Se il vostro ISP ha assegnato un Nome Host al vostro computer dovete inserirlo qui.
- **Indirizzo MAC:** L'indirizzo MAC (Media Access Control) è un codice identificativo unico per ogni interfaccia di rete. Alcuni ISP controllano gli indirizzi MAC dei dispositivi di rete che tentano di connettersi al loro servizio e rifiutano ogni richiesta proveniente da dispositivi di cui non sono a conoscenza. Per evitare problemi di questo tipo dovuti a indirizzi MAC non registrati potete:
  - Contattare il vostro ISP e aggiornare l'elenco degli indirizzi MAC associati al vostro servizio.
  - Clonare o modificare l'indirizzo MAC del vostro router ASUS in modo che sia uguale all'indirizzo MAC del vostro precedente router.
- **Frequenza query DHCP:** Cambia l'intervallo di DHCP Discovery per evitare sovraccarichi del server DHCP.

## 4.5.2 WAN duale

Il router wireless ASUS supporta la WAN duale. Potete impostare la WAN duale secondo una delle due seguenti modalità:

- **Modalità failover:** Selezionate questa modalità per usare la WAN secondaria come accesso di riserva alla rete.
- **Modalità bilanciata:** Selezionate questa modalità per ottimizzare la banda, minimizzare il tempo di risposta e prevenire sovraccarico di dati per ciascuna delle due WAN.

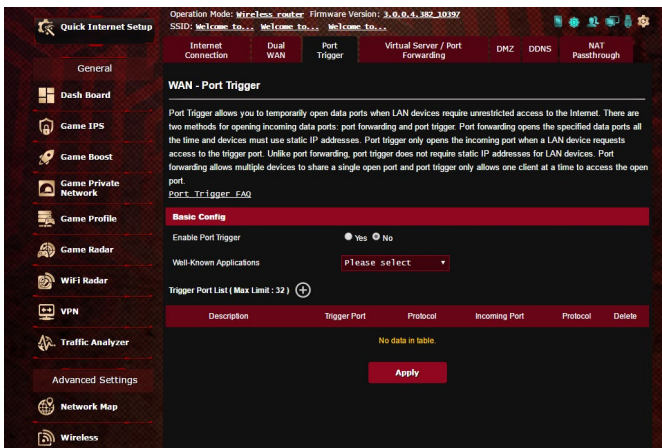




## 4.5.3 Port Trigger



Il trigger di un intervallo di porte apre una porta in ingresso predefinita per un periodo di tempo limitato quando un client della rete locale fa una richiesta di connessione in uscita relativamente ad una porta specifica. Il Port Trigger si usa nei seguenti casi:

- Diversi client della rete locale hanno bisogno di port forwarding per la stessa applicazione contemporaneamente.
- Un'applicazione richiede una specifica porta in ingresso diversa dalla porta in uscita.



### Per configurare il Port Trigger:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate)** > **WAN** e selezionate la scheda **Port Trigger**.
2. Selezionate **Yes (Sì)** alla voce **Enable Port Trigger (Abilita Port Trigger)**.
3. Nel campo **Well-Known Applications (Applicazioni più comuni)** selezionate i servizi web e i giochi popolari da aggiungere all'elenco dei Port Trigger.

4. Nella tabella **Trigger Port List (Elenco Port Trigger)** inserite le seguenti informazioni
  - **Descrizione:** Inserite un nome o una descrizione del servizio.
  - **Porta Trigger:** Specificate la porta trigger che intendete usare.
  - **Protocollo:** Selezionate il protocollo, TCP o UDP.
  - **Porta in ingresso:** Inserite una porta in ingresso per ricevere traffico in ingresso da Internet.
  - **Protocollo:** Selezionate il protocollo, TCP o UDP.
5. Cliccate sul pulsante **Add (Aggiungi)**  per inserire le informazioni per la porta trigger nell'elenco. Cliccate sul pulsante **Delete (Elimina)**  per rimuovere una porta trigger dall'elenco.
6. Quando avete finito cliccate su **Apply (Applica)**.

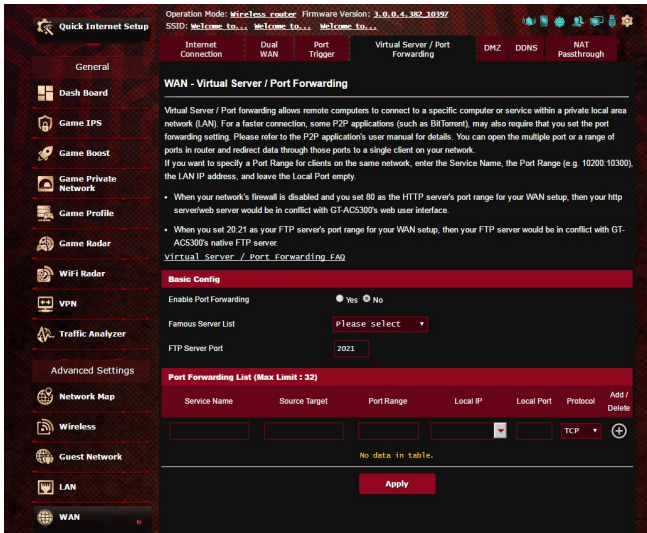
---

**NOTE:**

- Quando vi connettete ad un server IRC un PC client stabilisce una connessione in uscita usando l'intervallo di porte trigger 6666-7000. Il server IRC risponde verificando il nome utente e creando una nuova connessione verso il PC client usando una porta in ingresso.
  - Se il Port Trigger è disabilitato il router chiude la connessione perché non è in grado di stabilire quale PC stia richiedendo accesso al servizio IRC. Quando il Port Trigger è abilitato il router assegna una porta in ingresso al client per ricevere il traffico in ingresso. La porta in ingresso viene chiusa dopo che è passato un determinato periodo di tempo perché il router non è a conoscenza di quando l'applicazione è stata chiusa.
  - Il Port Triggering permette solo ad un client della rete di usare un particolare servizio tramite una particolare porta in un periodo di tempo specifico.
  - Non potete usare la stessa applicazione per attivare una porta in più di un PC allo stesso momento. La porta sarà inoltrata solamente all'ultimo client che ha mandato al router una richiesta di trigger.
-

## 4.5.4 Virtual Server / Port Forwarding

Il Port Forwarding è un metodo per dirigere il traffico di rete da Internet ad una porta specifica, o ad un intervallo specifico di porte, verso un client della vostra rete locale. Il servizio di Port Forwarding permette ai PC all'esterno della vostra rete locale di accedere a servizi specifici forniti da un PC all'interno della vostra rete locale.



### Per configurare il Port Forwarding:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > WAN** e selezionate la scheda **Virtual Server / Port Forwarding**.
2. Selezionate **Yes (Sì)** alla voce **Enable Port Forwarding (Abilita Port Forwarding)**.
3. Nel campo **Famous Server List (Servizi più comuni)** selezionate il tipo di servizio al quale volete accedere.
4. Nel campo **Famous Game List (Giochi più comuni)** selezionate il gioco al quale volete accedere. Questa voce elenca le porte richieste dai giochi più popolari.

5. Nella tabella **Port Forwarding List (Elenco Port Forwarding)** inserite le seguenti informazioni:

- **Nome del servizio:** Inserite il nome del servizio.
- **Intervallo porte:** Se volete specificare un intervallo di porte per i client della stessa rete inserite il nome del servizio, l'intervallo di porte (ad esempio 10200:10300), l'indirizzo IP della LAN, e lasciate vuoto il campo Porta locale. Questo campo accetta vari formati come, ad esempio, un intervallo di porte (300:350), porte singole (566,789) o misto (1015:1024,3021).

---



**NOTE:**

- Quando il firewall di rete è disabilitato e voi selezionate la porta 80 come predefinita per il vostro server HTTP lo stesso server andrà in conflitto con l'interfaccia web di gestione del router.
- Una rete utilizza il concetto di porta in modo da scambiare dati seguendo il principio che ogni porta sia assegnata ad un servizio ben preciso. Per esempio il servizio HTTP usa la porta 80. Ogni porta può essere usata per un solo servizio alla volta. Di conseguenza, se due PC tentano di accedere ai dati attraverso la stessa porta, il processo fallirà. Quindi, ad esempio, ecco perché non potete configurare il servizio di Port Forwarding sulla porta 100 contemporaneamente per due PC della stessa rete.

- 
- **IP Locale:** Inserite l'indirizzo IP locale del client.

---

**NOTA:** Assicuratevi che il client disponga di un indirizzo IP statico per fare in modo che il port-forwarding funzioni correttamente. Fate riferimento alla sezione «4.4 LAN» per maggiori informazioni.

- 
- **Porta locale:** Inserite una porta specifica per ricevere i pacchetti inoltrati. Lasciate vuoto questo campo se volete che i pacchetti siano diretti al range specifico di porte.
  - **Protocollo:** Selezionate il protocollo. Se non siete sicuri selezionate **BOTH (ENTRAMBI)**.
6. Cliccate sul pulsante **Add (Aggiungi)**  per inserire le informazioni per la porta trigger nell'elenco. Cliccate sul pulsante **Delete (Elimina)**  per rimuovere una porta trigger dall'elenco.

7. Quando avete finito cliccate su **Apply (Applica)**.

**Per controllare che il Port Forwarding sia configurato correttamente:**

- Assicuratevi che il vostro server, o l'applicazione, siano avviati e operativi.
- Avete bisogno di un client al di fuori della vostra rete LAN (Internet client). Questo client non deve essere connesso al router ASUS.
- Dall'Internet client usate l'indirizzo IP pubblico (WAN) del router per accedere al servizio. Se il port forwarding è stato configurato correttamente dovrete essere in grado di accedere ai file e alle applicazioni.

**Differenze tra port trigger e port forwarding**

- Il Port Trigger funziona anche senza bisogno di inserire un indirizzo IP LAN specifico. A differenza del port forwarding, il quale richiede un indirizzo IP statico sulla LAN, il port trigger permette un reindirizzamento dinamico. Range di porte predeterminati sono configurati per accettare connessioni in ingresso per un breve periodo di tempo. Il port trigger permette a diversi computer di accedere a programmi che, normalmente, richiederebbero un port forwarding manuale per ogni client della rete.
- Il port trigger è più sicuro del port forwarding dal momento che le porte in ingresso non sono aperte in modo continuo. Le porte vengono aperte solamente quando l'applicazione stabilisce una connessione in uscita attraverso la porta di trigger.

## 4.5.5 DMZ

Il servizio DMZ espone un client della rete direttamente ad Internet permettendogli di ricevere tutti i pacchetti in entrata diretti alla vostra rete locale.

Il traffico in ingresso, di solito, è diretto ad un client specifico della rete solamente se una regola di port-forwarding per una specifica porta è stata configurata sul router, altrimenti viene scartato. In una configurazione DMZ uno specifico client della rete riceve tutti i pacchetti in ingresso.

La configurazione DMZ è utile quando si ha bisogno di avere le porte in ingresso aperte verso l'esterno perché, ad esempio, si intende ospitare un server di dominio, web o email.

---

**ATTENZIONE:** L'apertura di tutte le porte in ingresso verso un client rende la rete locale vulnerabile agli attacchi dall'esterno. Siate quindi consapevoli dei rischi a cui andate incontro se decidete di usare il servizio DMZ.

---

### Per configurare DMZ:

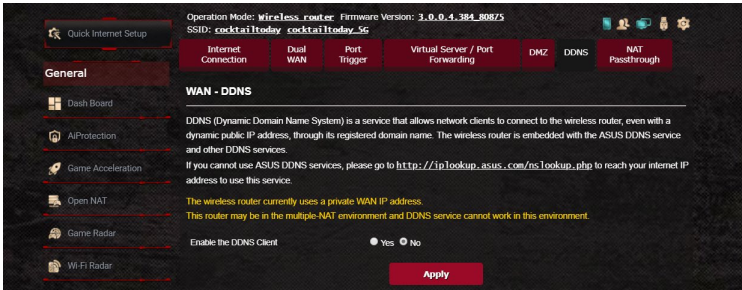
1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate)** > **WAN** e selezionate la scheda **DMZ**.
2. Configurate le seguenti impostazioni. Quando avete finito cliccate su **Apply (Applica)**.
  - **Indirizzo IP del client bersaglio:** Inserite l'indirizzo IP (relativo alla rete locale) del client per il quale volete attivare il servizio DMZ in modo da esporlo alla rete Internet. Assicuratevi che il client disponga di un indirizzo IP statico.

### Per disabilitare DMZ:

1. Eliminate l'indirizzo IP del client dalla casella di testo **IP Address of Exposed Station (Indirizzo IP del client bersaglio)**.
2. Quando avete finito cliccate su **Apply (Applica)**.

## 4.5.6 DNS Dinamico

Configurando il servizio DNS dinamico (DDNS) avrete la possibilità di accedere al router dall'esterno della vostra rete. Potete scegliere di usare il servizio ASUS DDNS (incluso) oppure un altro servizio DDNS.



**Per configurare un DNS Dinamico:**

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > WAN** e selezionate la scheda **DNS Dinamico**.
2. Configurate le seguenti impostazioni. Quando avete finito cliccate su **Apply (Applica)**.
  - **Enable the DDNS Client (Abilita il client DDNS):** Abilita l'accesso al router ASUS dall'esterno tramite nome DNS piuttosto che per indirizzo IP pubblico.
  - **Server and Host Name (Server e Nome Host):** Scegliete ASUS DDNS o un altro DDNS. Se volete usare ASUS DDNS inserite il Nome Host nel formato xxx.asuscomm.com (dove xxx è il vostro Nome Host).
  - Se volete usare un servizio DDNS diverso selezionatelo dall'elenco, cliccate su **Free Trial (Prova gratuita)** e registratevi online prima di usare il servizio. Compilate i campi **Nome utente** o **Indirizzo email** e **Password o chiave DDNS**.
  - **Enable wildcard (Abilita wildcard):** Abilitate le wildcard (metacaratteri) se il vostro server DNS Dinamico lo richiede.

## NOTE:

Il server DNS Dinamico non funzionerà nei seguenti casi:

- Quando il router usa come indirizzo pubblico (WAN) un indirizzo IP destinato alle reti private (192.168.x.x, 10.x.x.x, or 172.16.x.x) come indicato dalla scritta in giallo.
- Il router si trova in una rete che usa NAT multipli.

## 4.5.7 NAT Passthrough

Il NAT Passthrough permette alla connessione VPN di passare attraverso i router e arrivare ai clienti di rete. Le modalità PPTP Passthrough, L2TP Passthrough, IPsec Passthrough e RTSP Passthrough sono abilitate di default.

Per abilitare / disabilitare le funzionalità NAT Passthrough andate su **Advanced Settings (Opzioni avanzate) > WAN** e selezionate la scheda **NAT Passthrough**. Quando avete finito cliccate su **Apply (Applica)**.

Operation Mode: Wireless Router Firmware Version: 3.0.0.4.384\_88875  
SSID: cocktailtoday cocktailtoday\_5G

Internet Connection Dual WAN Port Trigger Virtual Server / Port Forwarding DMZ DDNS NAT Passthrough

### WAN - NAT Passthrough

Enable NAT Passthrough to allow a Virtual Private Network (VPN) connection to pass through the router to the network clients.

PPTP Passthrough	Enable
L2TP Passthrough	Enable
IPSec Passthrough	Enable
RTSP Passthrough	Enable
H.323 Passthrough	Enable
SIP Passthrough	Enable
PPPoE Relay	Disable
FTP_ALG Port	2021

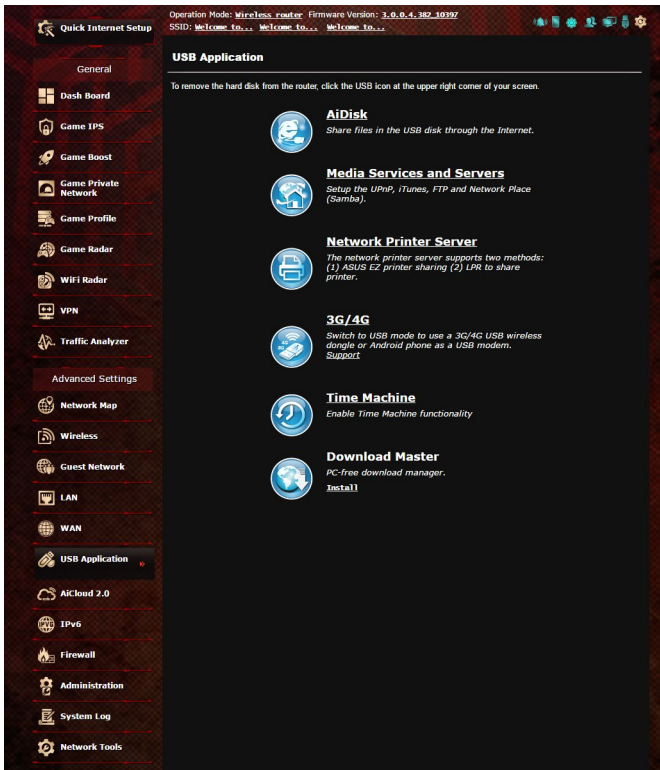
Apply



## 4.6 Utilizzare le Applicazioni USB

Il menu Applicazioni USB fornisce le funzioni AiDisk, Gestione Server, Server di stampa di rete e il Download Master.

**IMPORTANTE!** Per usare le funzioni server è necessario inserire un dispositivo di archiviazione USB, come un hard disk USB o una memoria flash USB, nella porta USB 2.0 del pannello posteriore del vostro router wireless. Assicuratevi che il dispositivo di archiviazione USB sia formattato e partizionato correttamente. Fate riferimento al sito web ASUS: <http://event.asus.com/2009/networks/disksupport/> per ottenere l'elenco dei file system compatibili.

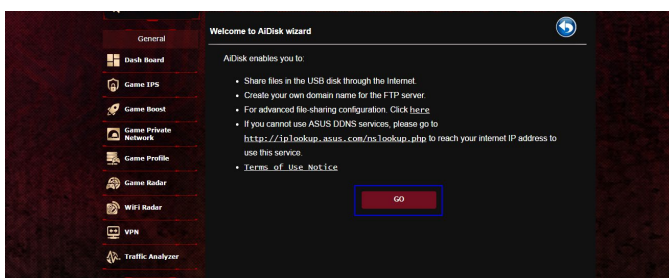


## 4.6.1 Usare AiDisk

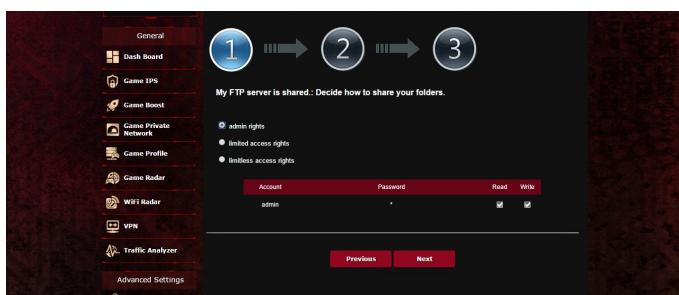
AiDisk vi permette di condividere file memorizzati su un dispositivo USB attraverso la rete Internet. AiDisk, inoltre, vi assiste nella configurazione di ASUS DDNS e del server FTP.

### Per usare AiDisk:

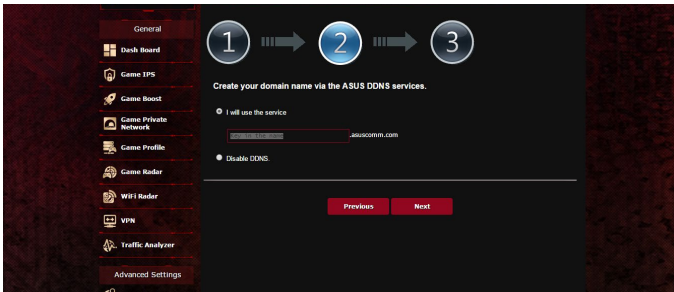
1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > USB Application (Applicazioni USB)** e poi cliccate sull'icona di **AiDisk**.
2. Nella pagina iniziale di configurazione guidata di AiDisk cliccate su **GO (Vai)**.



3. Selezionate i permessi di accesso che volete attribuire ai client che accedono ai vostri dati condivisi.



4. Create il vostro nome di dominio tramite il servizio ASUS DDNS, leggete le Condizioni per l'utilizzo del servizio, selezionate **I will use the service and accept the Terms of service (Userò il servizio ed accetto le Condizioni per l'utilizzo del servizio)** e inserite il vostro nome di dominio. Quando avete finito cliccate su **Next (Avanti)**.



- Potete anche scegliere l'opzione **Skip ASUS DDNS settings (Salta configurazione ASUS DDNS)**, e cliccare su **Next (Avanti)**, per saltare la configurazione del DNS Dinamico.
5. Cliccate su **Finish (Fine)** per completare la configurazione.
  6. Per accedere al server FTP che avete creato inserite il link FTP **ftp://<domain name>.asuscomm.com** in un browser web o in un programma client FTP.

## 4.6.2 Usare Gestione Server

Gestione Server vi permette di condividere file multimediali da un disco USB tramite una cartella impostata sul Server multimediale e usando il servizio di Condivisione Samba o la Condivisione FTP. In Gestione Server potete anche configurare altre impostazioni per il disco USB.

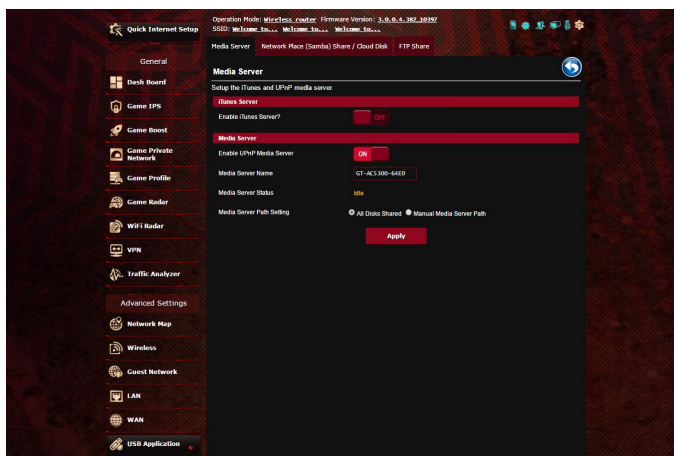
### Utilizzare il Server multimediale

Il vostro router wireless permette ai dispositivi compatibili DLNA di accedere ai file multimediali presenti sul disco USB collegato al vostro router wireless.

---

**NOTA:** Prima di poter utilizzare la funzione Server multimediale DLNA dovete connettere il vostro dispositivo alla rete gestita dal router.

---



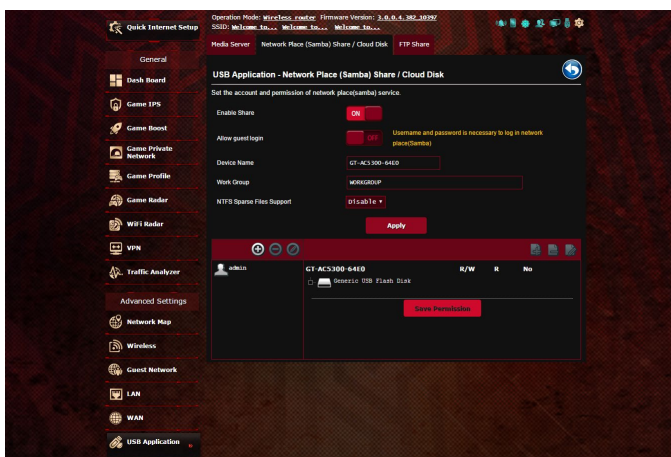
Per lanciare le impostazioni del Server multimediale andate su **Advanced Settings (Impostazioni avanzate) > USB Application (Applicazioni USB) > Media Services and Servers (Servizi e server multimediale)** e selezionate la scheda **Media Servers (Server multimediale)**. Fate riferimento alle seguenti informazioni in merito alle diverse voci presenti nel menu:

- **Enable iTunes Server (Abilitare il server iTunes)?:** Spostate il cursore su ON/OFF per abilitare/disabilitare il Server iTunes.

- **Enable DLNA Media Server (Abilita Server multimediale DLNA):** Spostate il cursore su ON/OFF per abilitare/disabilitare il Server multimediale DLNA.
- **Media Server Status (Stato Server multimediale):** Visualizza lo stato corrente del Server multimediale.
- **Impostazioni percorso Server multimediale:** Selezionate **All Disks Shared (Tutti i dischi condivisi)** o **Manual Media Server Path (Percorso manuale Server multimediale)**.

## Utilizzare la Condivisione Risorse di rete (Samba)

La Condivisione Risorse di rete (Samba) vi permette di impostare gli utenti e i permessi per il servizio Samba.



### Per usare Condivisione Samba:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > USB Application (Applicazioni USB) > Media Services and Servers (Servizi e server multimediale)** e selezionate la scheda **Network Place (Samba) Share / Cloud Disk (Condivisione Risorse di rete (Samba) / Disco Cloud)**.


---

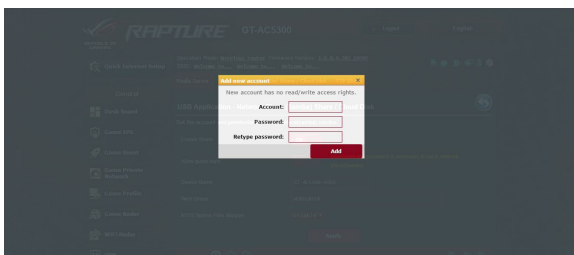
**NOTA:** Condivisione Samba, per la rete locale, è abilitata di default.

---


2. Per aggiungere, eliminare o modificare un account procedete nei modi seguenti.

### Per creare un nuovo account:


- a) Cliccate su  per aggiungere un nuovo account.
- b) Nei campi **Account** e **Password** inserite il nome utente e la password del vostro account. Riscrivete la password per confermare. Cliccate su **Add (Aggiungi)** per aggiungere l'utente all'elenco.

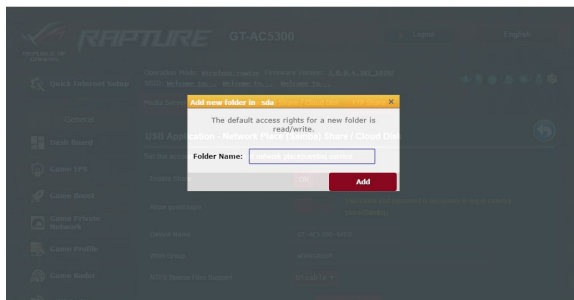


### Per eliminare un account esistente:

- a) Selezionate l'account che volete eliminare.
- b) Cliccate su .
- c) Quando richiesto cliccate su **Delete (Elimina)** per confermare la cancellazione dell'account.

### Per aggiungere una cartella:

- a) Cliccate su .
- b) Inserite il nome della cartella e cliccate su **Add (Aggiungi)**. La cartella che avete appena creato sarà aggiunta all'elenco delle cartelle.



3. Nell'elenco delle cartelle selezionate i permessi di accesso che volete assegnare alle cartelle specifiche:
  - **R/W**: Selezionate per impostare i permessi di lettura (R) e scrittura (W).
  - **R**: Selezionate per impostare i permessi di sola lettura.
  - **No**: Selezionate questa opzione se non volete condividere una cartella specifica.
4. Cliccate su **Apply (Applica)** per confermare le modifiche.

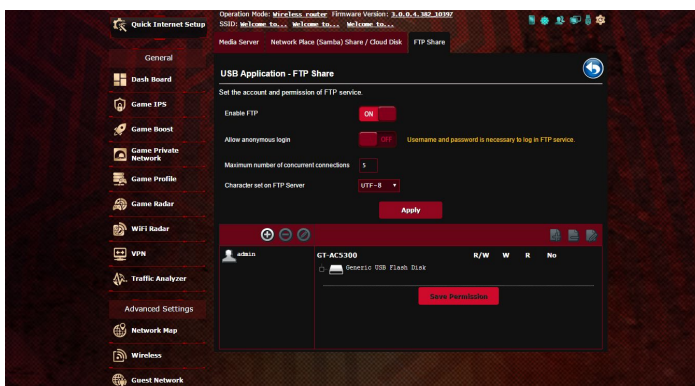
## Utilizzare il servizio FTP Share (Condivisione FTP)

Condivisione FTP permette ad un server FTP di condividere file da un disco USB ad altri dispositivi connessi alla vostra rete locale o ad Internet.

---

### IMPORTANTE:

- Assicuratevi di aver fatto una rimozione sicura del disco USB. Una rimozione non corretta del disco USB potrebbe causare perdite di dati.
  - Per rimuovere correttamente il vostro disco USB fate riferimento alla sezione «Rimozione sicura del disco USB» del paragrafo «4.1.3 Controllo del vostro dispositivo USB».
- 



## Per usare il servizio FTP Share (Condivisione FTP):

---

**NOTA:** Assicuratevi di aver abilitato il server FTP di AiDisk. Per maggiori dettagli fate riferimento alla sezione «4.6.1 Usare AiDisk».

---

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > USB Application (Applicazioni USB) > Media Services and Servers (Servizi e server multimediale)** e selezionate la scheda **FTP Share (Condivisione FTP)**.
2. Nell'elenco delle cartelle selezionate i permessi di accesso che volete assegnare alle cartelle specifiche
  - **R/W:** Selezionate per impostare i permessi di lettura (R) e scrittura (W) per la cartella specifica.
  - **S:** Selezionate per impostare i permessi di sola scrittura per una cartella specifica.
  - **R:** Selezionate per impostare i permessi di sola lettura per una cartella specifica.
  - **No:** Selezionate questa opzione se non volete condividere una cartella specifica.
3. Se preferite potete impostare il valore **ON** alla voce **Allow anonymous login (Permetti accesso anonimo)**.
4. Nel campo **Maximum number of concurrent connections (Numero massimo di connessioni simultanee)** inserite il numero massimo di dispositivi che possono connettersi simultaneamente al server FTP.
5. Cliccate su **Apply (Applica)** per confermare le modifiche.
6. Per accedere al server FTP inserite il link FTP **ftp://<hostname>.asuscomm.com** in un browser web o in un programma client FTP. Quando la connessione sarà effettuata vi sarà richiesto il nome utente e la password di accesso.



### 4.6.3 3G/4G

Diversi modem 3G/4G possono essere collegati al router per fornire accesso ad Internet.

---

**NOTA:** Per un elenco dei modem USB supportati visitate il sito: <http://event.asus.com/2009/networks/3gsupport/>

---

#### Per configurare l'accesso ad Internet 3G/4G:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > USB Application (Applicazioni USB) > 3G/4G**.
2. Alla voce **Enable USB Modem (Abilita modem USB)** selezionate **Yes (Sì)**.
3. Configurate le seguenti opzioni:
  - **Location (Posizione):** Selezionate la posizione del vostro service provider 3G/4G dall'elenco.
  - **ISP:** Selezionate il vostro ISP (Internet Service Provider) dall'elenco.
  - **APN (Access Point Name) service (Servizio APN):** Contattate il vostro service provider 3G/4G per maggiori informazioni.
  - **Dial Number and PIN code (Numero da comporre e codice PIN):** Il numero da comporre per accedere al servizio 3G/4G e il codice PIN.

---

**NOTA:** Il codice PIN potrebbe variare a seconda del vostro fornitore di servizi Internet.

---

- **Username / Password (Nome utente / Password):** Il **nome utente** e la **password** sono fornite dal vostro operatore 3G/4G.
  - **Modem USB:** Scegliete il modello del vostro modem USB 3G/4G dall'elenco a disposizione. Se non siete sicuri del modello selezionate **Auto (Automatico)**.
4. Cliccate su **Apply (Applica)**.

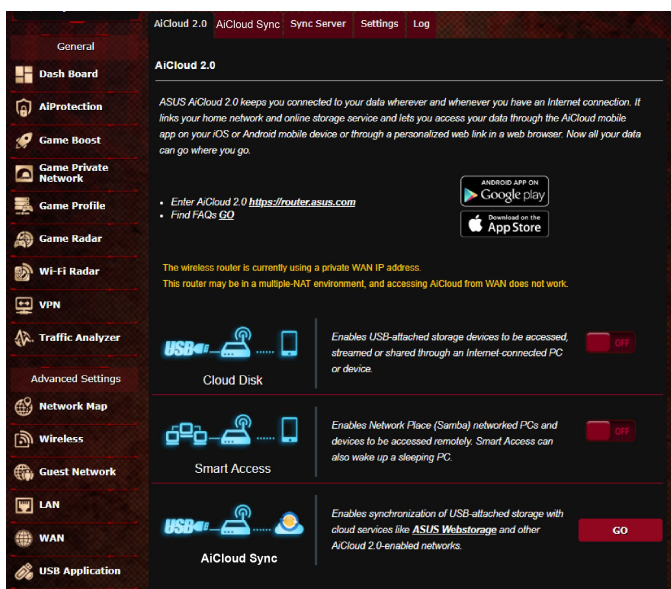
---

**NOTA:** Il router si riavvia automaticamente per attivare le impostazioni.

---

## 4.7 Utilizzo di AiCloud 2.0

AiCloud 2.0 è un servizio cloud che vi permette di salvare, sincronizzare, condividere e accedere ai vostri file.



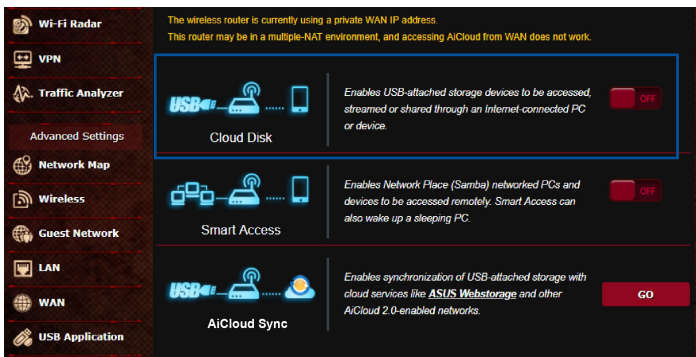
### Per usare AiCloud 2.0:

1. Dal Google Play Store, o dall'Apple Store, scaricate e installate sul vostro dispositivo mobile l'App ASUS AiCloud.
2. Connettete il vostro dispositivo mobile alla rete. Seguite le istruzioni per completare la configurazione di AiCloud.

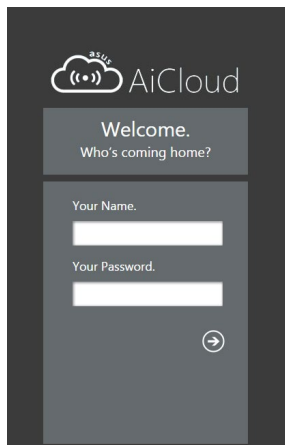
## 4.7.1 Disco Cloud

### Per creare un disco cloud:

1. Inserite un dispositivo di archiviazione USB nella porta USB del vostro router wireless.
2. Attivate **Cloud Disk** spostando il cursore su **ON**.



3. Andate su <https://router.asus.com> e inserite il nome utente e la password per l'accesso al router. Raccomandiamo di utilizzare **Google Chrome** o **Mozilla Firefox** per un'esperienza migliore.

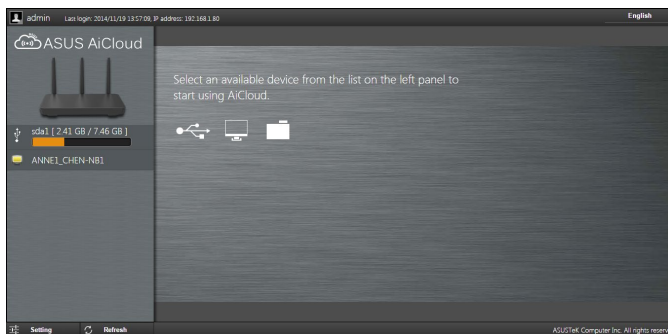


4. Potete ora avere accesso ai file presenti sui dischi cloud dei dispositivi connessi alla vostra rete.

---

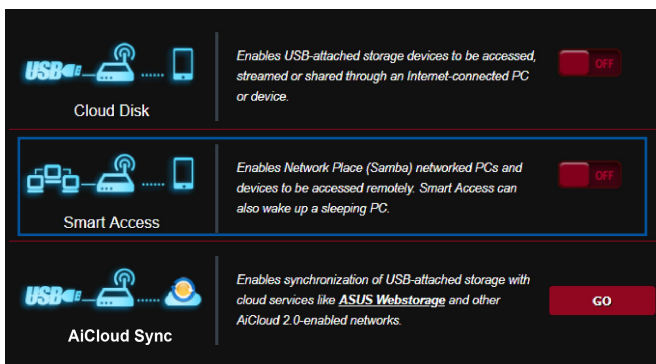
**NOTA:** Quando vorrete accedere ai dispositivi connessi alla rete avrete bisogno di inserire manualmente il nome utente e la password del singolo dispositivo. Questi dati non vengono salvati da AiCloud per ragioni di sicurezza.

---



## 4.7.2 Smart Access

La funzione Smart Access permette di accedere facilmente alla vostra rete domestica tramite il nome di dominio del vostro router.

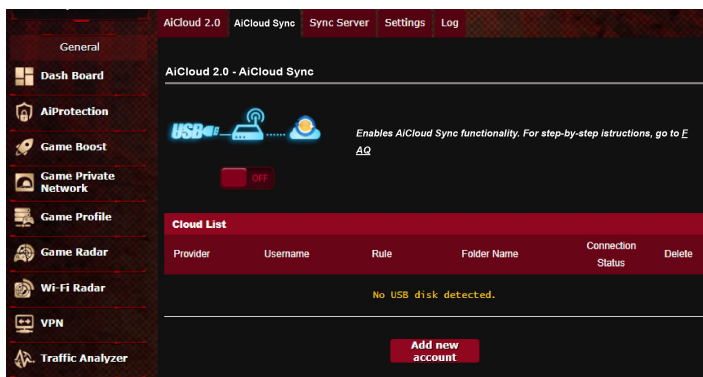


---

### NOTE:

- Potete creare un nome di dominio per il vostro router usando ASUS DDNS. Per maggiori dettagli fate riferimento alla sezione «4.5.6 DNS Dinamico».
  - Come impostazione standard AiCloud stabilisce una connessione sicura HTTPS. Inserite il vostro account [https://\[accountASUSDDNS\].asuscomm.com](https://[accountASUSDDNS].asuscomm.com) per un utilizzo sicuro di Cloud Disk e Smart Access.
-

## 4.7.3 AiCloud Sync

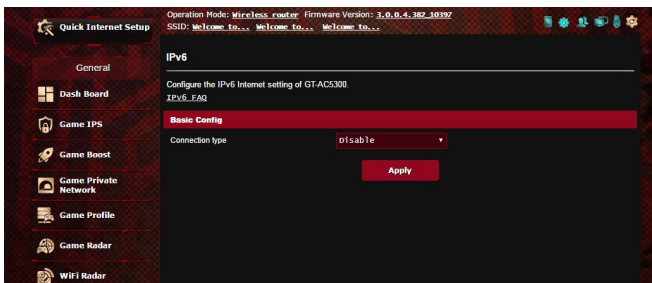


### Per usare AiCloud Sync:

1. Avviate AiCloud, andate su **AiCloud Sync** e cliccate su **Go (Vai)**.
2. Spostate il cursore su **ON** per abilitare AiCloud Sync.
3. Cliccate su **Add new account (Aggiungi nuovo account)**.
4. Inserite il nome utente e la password del vostro account ASUS WebStorage e selezionate la directory che volete mantenere sincronizzata con WebStorage.
5. Cliccate su **Apply (Applica)**.

## 4.8 IPv6

Il router wireless supporta il protocollo IPv6, un protocollo in grado di gestire molti più indirizzi del protocollo IPv4. Questo standard non è ancora disponibile in maniera molto diffusa. Chiedete informazioni al vostro ISP per sapere se IPv6 è effettivamente supportato.



### Per configurare IPv6:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > IPv6**.
2. Selezionate il **Connection Type (Tipo di connessione)** appropriato. Le opzioni di configurazione variano a seconda del tipo di connessione selezionata.
3. Inserite le impostazioni della LAN IPv6 e del server DNS.
4. Cliccate su **Apply (Applica)**.

---

**NOTA:** Chiedete informazioni al vostro ISP per sapere se IPv6 è effettivamente supportato.

---

## 4.9 Firewall

Il router wireless può funzionare anche da firewall hardware per la vostra rete.

---

**NOTA:** La funzione Firewall è abilitata su tutti i router.

---

### 4.9.1 Generale

**Per configurare le impostazioni di base del firewall:**

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate)** > **Firewall** e selezionate la scheda **General (Generale)**.
2. Alla voce **Enable Firewall (Abilita Firewall)** selezionate **Yes (Sì)**.
3. Alla voce **Enable DoS protection (Abilita la protezione DoS)** selezionate **Yes (Sì)** se volete proteggere la vostra rete da possibili attacchi DoS (Denial of Service) che possono peggiorare notevolmente le prestazioni del vostro router.
4. Potete anche controllare i pacchetti scambiati tra LAN (rete locale) e WAN (Internet). Alla voce **Logged packets type (Tipologia di pacchetti registrati)** selezionate **Dropped (Scartati)**, **Accepted (Accettati)** o **Both (Entrambi)**.
5. Cliccate su **Apply (Applica)**.

### 4.9.2 Filtro URL

Potete specificare parole chiave o indirizzi web per impedire l'accesso a URL specifici.


---

**NOTA:** Il filtro URL lavora sulle query DNS. Se un client ha già effettuato l'accesso ad un sito web, ad esempio <http://www.abcxxx.com>, potrà comunque visitare nuovamente il sito anche se il filtro lo impedirebbe (la cache DNS del sistema ricorda i siti visitati in precedenza in modo da non dover continuamente interrogare il server DNS). Per risolvere questo problema svuotate la cache DNS prima di impostare il filtro URL.

---

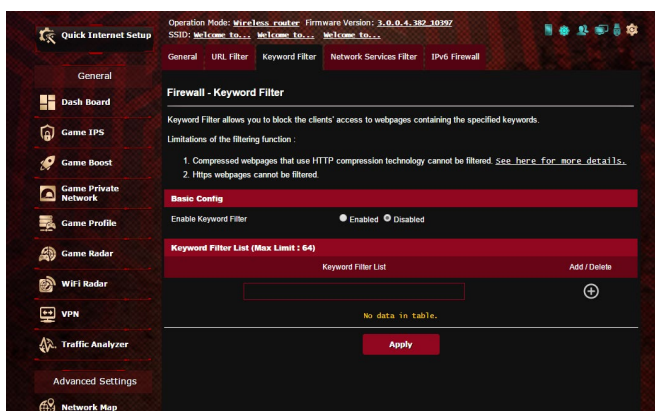


### **Per abilitare e configurare il filtro URL:**

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Firewall** e selezionate la scheda **URL filter (Filtro URL)**.
2. Alla voce **Enable URL Filter (Abilita filtro URL)** selezionate **Enable (Abilita)**.
3. Inserite un indirizzo Internet e cliccate sul pulsante .
4. Cliccate su **Apply (Applica)**.

## 4.9.3 Filtro Parole Chiave

Il Filtro Parole Chiave blocca l'accesso alle pagine web contenenti le parole che inserite nell'elenco.



### Per abilitare e configurare il Filtro Parole Chiave:

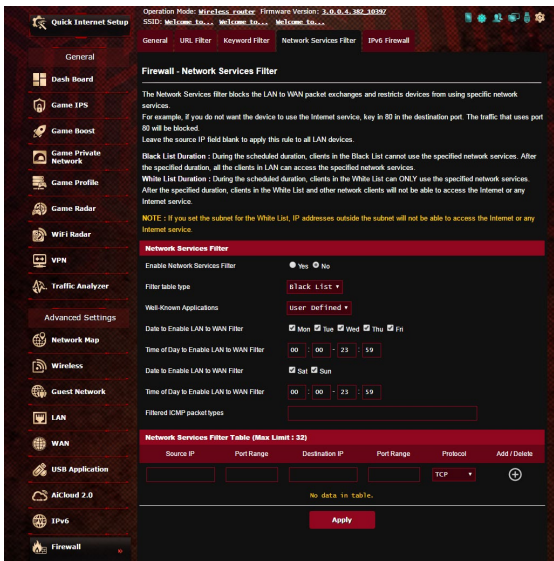
1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Firewall** e selezionate la scheda **Keyword Filter (Filtro parole chiave)**.
2. Alla voce **Enable Keyword Filter (Abilita Filtro Parole Chiave)** selezionate **Enable (Abilita)**.
3. Inserite una parola o una frase e poi cliccate sul pulsante **Add (Aggiungi)**.
4. Cliccate su **Apply (Applica)**.

### NOTE:

- Il Filtro Parole Chiave lavora sulle query DNS. Se un client ha già effettuato l'accesso ad un sito web, ad esempio <http://www.abcxxx.com>, potrà comunque visitare nuovamente il sito anche se il filtro lo impedirebbe (la cache DNS del sistema ricorda i siti visitati in precedenza in modo da non dover continuamente interrogare il server DNS). Per risolvere questo problema svuotate la cache DNS prima di impostare il Filtro Parole Chiave.
- Le pagine web compresse tramite la compressione HTTP non possono essere filtrate. Neanche le pagine HTTPS possono essere bloccate tramite il Filtro Parole Chiave.

## 4.9.4 Packet Filter

Il Packet Filter blocca i pacchetti diretti verso l'esterno della rete e limita l'accesso dei client di rete a servizi specifici come Telnet o FTP.



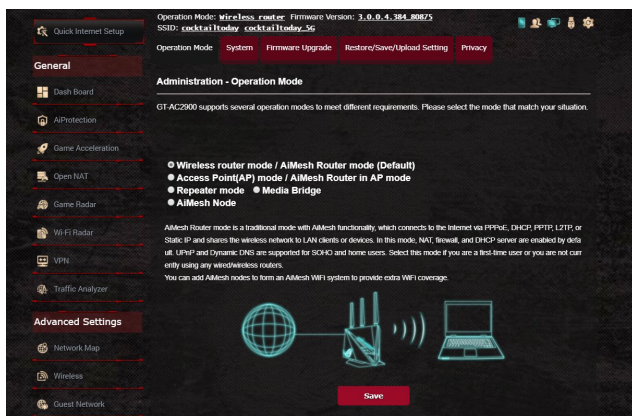
### Per abilitare e configurare il Packet Filter:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Administration (Amministrazione)** e selezionate la scheda **Network Service Filter (Packet Filter)**.
2. Alla voce **Enable Network Services Filter (Abilita Packet Filter)** selezionate **Yes (Sì)**.
3. Selezionate la modalità di filtraggio. **Black List** blocca i servizi di rete selezionati. **Lista consentiti** limita l'accesso esclusivamente ai servizi selezionati.
4. Selezionate giorno e orario nei quali intendete attivare il filtro.
5. Per aggiungere un nuovo servizio da filtrare inserite IP sorgente, IP destinazione, porta/e e il protocollo. Cliccate sul pulsante **+**.
6. Cliccate su **Apply (Applica)**.

## 4.10 Amministrazione

### 4.10.1 Modalità operativa

La pagina **Modalità operativa** vi permette di scegliere la modalità appropriata necessaria per la vostra rete.



**Per impostare la modalità operativa:**

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Administration (Amministrazione)** e selezionate la scheda **Operation Mode (Modalità operativa)**.
2. Selezionate una delle seguenti modalità operative:
  - **Wireless router mode (default) (Modalità router wireless (predefinita)):** Nella modalità router wireless il router wireless si connette a Internet e fornisce accesso ad Internet a tutti i dispositivi presenti nella sua rete locale.
  - **Access Point mode (Modalità Access Point):** In questo modo il router, collegato ad una rete cablata, crea una nuova rete wireless.
  - **Media Bridge:** Questa configurazione richiede due router wireless. Il secondo router, configurato come media bridge, permette la connessione prioritaria di dispositivi come Smart TV o console di gioco tramite interfaccia Ethernet.
  - **Repeater Mode (Modalità ripetitore):** Nella modalità ripetitore GT-AC2900 si connette in modalità wireless ad un altro router wireless per estendere la copertura wireless.

In questa modalità le funzioni firewall, IP sharing e NAT sono disabilitate.

- **Modalità AiMesh:** Questa modalità richiede almeno due router ASUS che supportano AiMesh. Abilitate il nodo AiMesh quindi eseguite l'accesso al router AiMesh per cercare i nodi AiMesh disponibili nelle vicinanze e aggiungerli al sistema AiMesh. Il sistema AiMesh fornisce una copertura completa dell'abitazione e gestione centralizzata.
3. Cliccate su **Apply (Applica)**.

---

**NOTA:** Il router si riavvia automaticamente per cambiare la modalità.

---

## 4.10.2 Sistema

La pagina **Sistema** vi permette di configurare le impostazioni del vostro router wireless.

### Per configurare le impostazioni di sistema:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Administration (Amministrazione)** e selezionate la scheda **System (Sistema)**.
2. Potete configurare le seguenti impostazioni:
  - **Change router login password (Cambia le credenziali di accesso al router):** Potete cambiare la password e il nome utente del vostro router wireless inserendo un nuovo nome utente e una nuova password.
  - **Time Zone (Fuso Orario):** Selezionate il corretto fuso orario per la vostra rete.
  - **NTP Server (Server NTP):** Il router wireless può ottenere informazioni da un server NTP (Network time Protocol) per regolare automaticamente data e ora.
  - **Enable Telnet (Abilita Telnet):** Selezionate **Yes (Sì)** per permettere le connessioni al router tramite il protocollo Telnet. Selezionate **No** per impedirlo.
  - **Authentication Method (Metodo d'autenticazione):** Potete scegliere HTTP, HTTPS o entrambi per un accesso al router sicuro.

- **Enable Web Access from WAN (Abilita l'accesso all'interfaccia Web da Internet):** Selezionate **Yes (Sì)** per permettere la gestione del router tramite interfaccia Web anche dall'esterno della vostra rete. Selezionate **No** per impedirlo.
  - **Permetti solo indirizzi IP specifici:** Selezionate **Yes (Sì)** per creare un elenco di indirizzi IP ai quali permettere la gestione del router tramite interfaccia Web dall'esterno della vostra rete.
  - **Client List (Elenco client fidati):** Inserite qui l'elenco degli indirizzi IP esterni ai quali volete permettere l'accesso alle impostazioni del router. Questo elenco è utilizzabile solo selezionando **Yes (Sì)** alla voce **Only allow specific IP (Indirizzi IP fidati)**.
3. Cliccate su **Apply (Applica)**.

### 4.10.3 Aggiornamento firmware

---

**NOTA:** Scaricate l'ultimo firmware disponibile dal sito web ASUS:  
<http://www.asus.com>

---

#### Per aggiornare il firmware:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Administration (Amministrazione)** e selezionate la scheda **Firmware Upgrade (Aggiornamento firmware)**.
2. Dalla pagina **New Firmware File (Nuovo file firmware)** cliccate su **Choose File (Sfoglia)** per cercare il file del firmware che avete appena scaricato.
3. Cliccate su **Upload (Carica)** per aggiornare il firmware.

---

#### NOTE:

- Quando l'aggiornamento del firmware è completato aspettate qualche minuto per permettere al sistema di riavviarsi.
  - Se l'aggiornamento del firmware fallisce il router wireless entra automaticamente in modalità di **recupero** e il LED di alimentazione del pannello anteriore comincia a lampeggiare lentamente. Fate riferimento alla sezione «5.2 Firmware Restoration» per avere maggiori informazioni su come effettuare il recupero del firmware.
-

## 4.10.4 Ripristina/Salva/Carica Impostazioni

**Per ripristinare/salvare/caricare le impostazioni del router wireless:**

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Administration (Amministrazione)** e selezionate la scheda **Restore/Save/Upload Setting (Impostazione Ripristina/Salva/Carica)**.
2. Selezionate il processo che volete eseguire:
  - Cliccate su **Restore (Ripristina)** e poi su **OK** se volete ripristinare le impostazioni predefinite di fabbrica.
  - Cliccate su **Save (Salva)**, scegliete un percorso dove salvare il file e poi cliccate su **Save (Salva)** se volete salvare le impostazioni correnti del sistema.
  - Cliccate su **Choose File (Sfoggia)**, selezionate il vostro file e poi cliccate su **Upload (Carica)** se volete ripristinare le impostazioni che avete precedentemente salvato su un file.

---

**NOTA:** Se ci fossero dei problemi aggiornate il firmware all'ultima versione e configurate le nuove impostazioni. **NON** ripristinate le impostazioni predefinite del router.

---

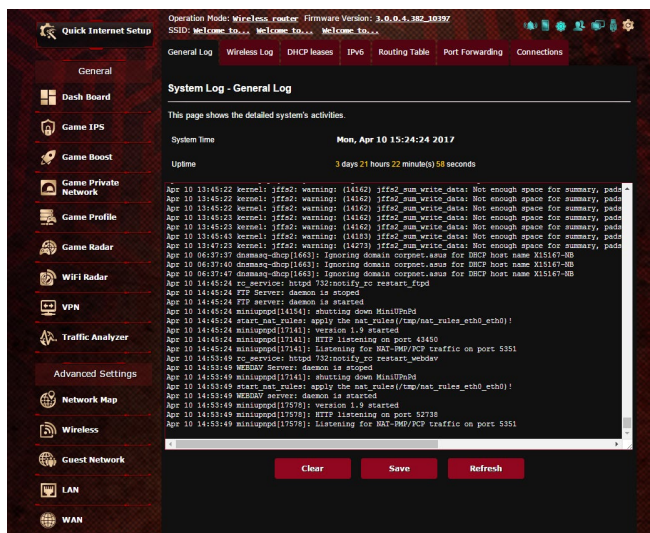
## 4.11 Registro di sistema

Il registro di sistema contiene la registrazione delle vostre attività di rete.

**NOTA:** Il registro di sistema viene cancellato quando il router viene riavviato o spento.

### Per visualizzare il vostro registro di sistema:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > System Log (Registro di sistema)**.
2. Potete visualizzare le diverse attività di rete in una delle seguenti schede:
  - General Log (Registro generale)
  - DHCP Leases (Lease DHCP)
  - Wireless Log (Registro wireless)
  - Port Forwarding
  - Routing Table (Tabella di routing)



The screenshot displays the 'System Log - General Log' interface of a router. The top navigation bar includes 'General Log', 'Wireless Log', 'DHCP leases', 'IPv6', 'Routing table', 'Port Forwarding', and 'Connections'. The main content area shows the system time as 'Mon, Apr 10 15:24:24 2017' and an uptime of '3 days 21 hours 22 minutes 58 seconds'. Below this, a scrollable log contains various system messages, including warnings about insufficient space for summaries, domain name resolution errors, and service startup logs for MiniUPnPd, dnsmasq, and WEBSAV.

```
Apr 10 13:45:22 kernel: jffs2: warning: (14162) jffs2_sum_write_data: Not enough space for summary, page
Apr 10 13:45:22 kernel: jffs2: warning: (14162) jffs2_sum_write_data: Not enough space for summary, page
Apr 10 13:45:23 kernel: jffs2: warning: (14162) jffs2_sum_write_data: Not enough space for summary, page
Apr 10 13:45:23 kernel: jffs2: warning: (14162) jffs2_sum_write_data: Not enough space for summary, page
Apr 10 13:45:23 kernel: jffs2: warning: (14162) jffs2_sum_write_data: Not enough space for summary, page
Apr 10 13:45:24 kernel: jffs2: warning: (14153) jffs2_sum_write_data: Not enough space for summary, page
Apr 10 13:47:23 kernel: jffs2: warning: (14273) jffs2_sum_write_data: Not enough space for summary, page
Apr 10 06:37:50 dnsmasq-dhcp[1663]: ignoring domain corpnet.asus for DHCP host name X15167-08
Apr 10 06:37:49 dnsmasq-dhcp[1663]: ignoring domain corpnet.asus for DHCP host name X15167-08
Apr 10 14:45:24 rc_service: httpd_732:notify_rc restart_fupd
Apr 10 14:45:24 FTP server: daemon is stopped
Apr 10 14:45:24 FTP server: daemon is started
Apr 10 14:45:24 miniupnpd[14154]: shutting down MiniUPnPd
Apr 10 14:45:51 nraas_nas_rules: apply the nas_rules/rtp/nas_rules_etcdb_etc01
Apr 10 14:45:24 miniupnpd[17141]: version 1.9 started
Apr 10 14:45:24 miniupnpd[17141]: HTTP listening on port 5350
Apr 10 14:45:24 miniupnpd[17141]: Listening for NAT-PMP/PCP traffic on port 5351
Apr 10 14:45:31 rc_service: httpd_732:notify_rc restart_webdav
Apr 10 14:45:31 WEBSAV server: daemon is stopped
Apr 10 14:45:31 miniupnpd[17141]: shutting down MiniUPnPd
Apr 10 14:45:31 nraas_nas_rules: apply the nas_rules/rtp/nas_rules_etcdb_etc01
Apr 10 14:45:31 WEBSAV server: daemon is started
Apr 10 14:45:31 miniupnpd[17178]: version 1.9 started
Apr 10 14:45:31 miniupnpd[17178]: HTTP listening on port 52738
Apr 10 14:45:31 miniupnpd[17178]: Listening for NAT-PMP/PCP traffic on port 5351
```



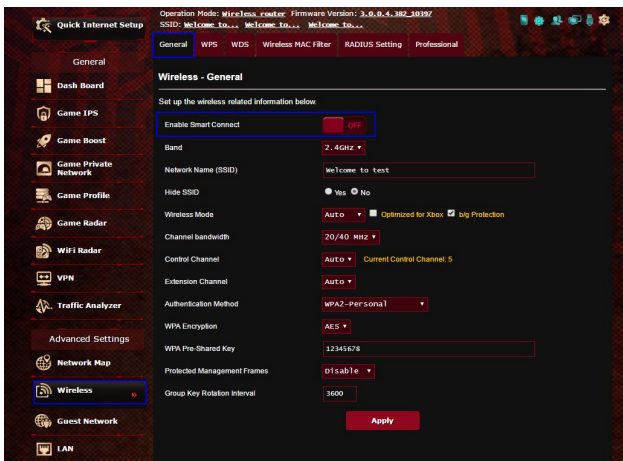
## 4.12 Smart Connect

Smart Connect è progettato per pilotare automaticamente i client a una delle tre frequenze disponibili (2.4 GHz, 5 GHz-1 o 5 GHz-2).

### 4.12.1 Configurazione di Smart Connect

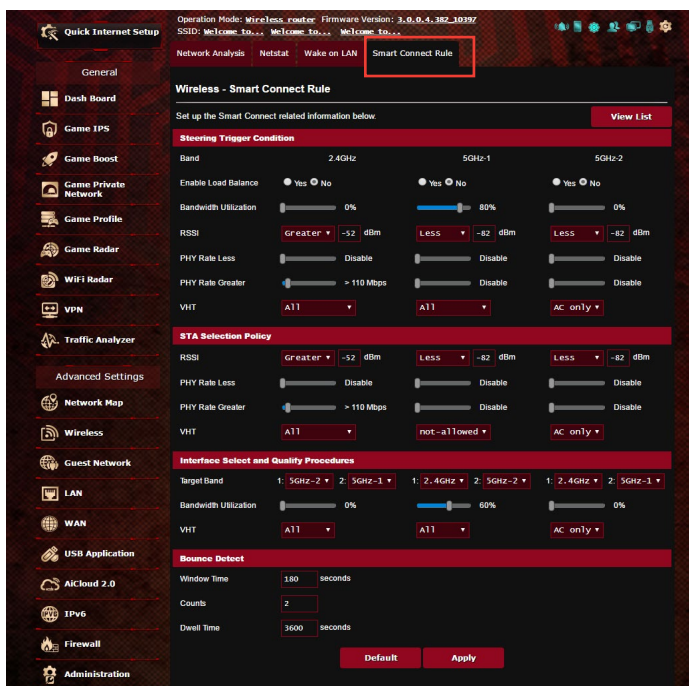
Potete abilitare Smart Connect dall'interfaccia web in uno dei seguenti modi:

- **Tramite la schermata Wireless**
  1. Avviate il vostro browser e inserite, nella barra degli indirizzi, l'indirizzo standard del router: <http://router.asus.com>.
  2. Nella pagina di login inserite il nome utente (**admin**) e la password (**admin**), poi cliccate su **OK**. La pagina dell'installazione rapida si carica automaticamente.
  3. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > Wireless** e selezionate la scheda **General (Generale)**.
  4. Spostatate su **ON** il cursore di **Enable Smart Connect (Abilita Smart Connect)**. Questa funzione connette automaticamente i client della vostra rete alla banda più appropriata per una velocità ottimale.



## 4.12.2 Regole di Smart Connect

ASUSWRT fornisce impostazioni predefinite standard per innescare i meccanismi interni. Potete anche cambiare le regole a seconda delle condizioni della vostra rete. Per cambiare le impostazioni andate sulla scheda **Smart Connect Rule (Regole di Smart Connect)** nella schermata degli strumenti di rete.

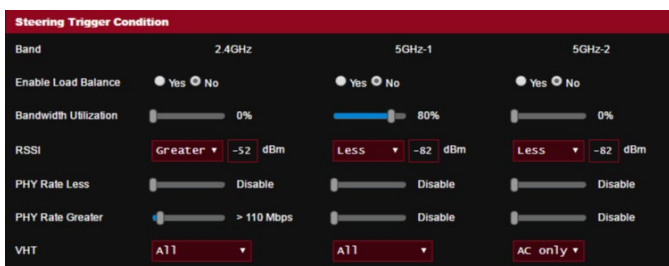


La scheda Regole di Smart Connect è divisa in quattro sezioni:

- Condizione steering trigger
- Regole di selezione STA
- Interface Select and Qualify Procedures (Selezione interfaccia e procedure di qualità)
- Rilevamento bounce

## Condizione steering trigger

Questo set di controlli permette di impostare i criteri per il controllo della banda.



- **Utilizzo banda**

Quando l'utilizzo della banda supera la percentuale impostata verrà innescato il cambiamento della banda.

- **Enable Load Balance**

Questa opzione controlla il bilanciamento del carico.

- **RSSI**

Se il livello del segnale ricevuto di uno qualsiasi dei client associati soddisfa questa condizione verrà innescato il cambiamento della banda.

- **PHY Rate Less / PHY Rate Greater**

Questi controlli determinano i livelli dei link STA che determinano il cambiamento della banda.

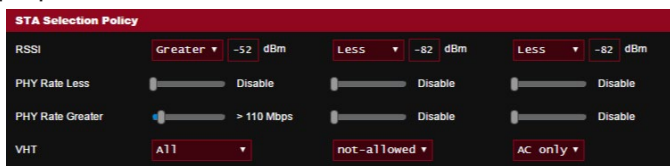
- **VHT**

Questi controlli determinano il modo in cui vengono gestiti i client 802.11ac e non-ac.

- **ALL (TUTTI)** (predefinito) tutti i client possono innescare il cambiamento.
- **Solo AC** un client deve supportare 802.11ac per innescare il cambiamento.
- **Not-allowed (Non permesso)** solo i client non-802.11ac potranno innescare il cambiamento, ad esempio 802.11a/b/g/n.

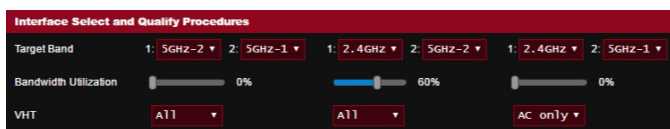
## Regole di selezione STA

Una volta innescato il cambiamento ASUSWRT si atterrà alle regole STA per selezionare il client (STA) che verrà indirizzato alla banda più appropriata.



## Interface Select and Qualify Procedures (Selezione interfaccia e procedure di qualità)

Questi controlli determinano il futuro del client che è stato reindirizzato in precedenza. I controlli **Target Band** permettono di specificare la prima e la seconda scelta per il cambiamento della banda. I client compatibili con i criteri delle regole STA verranno indirizzati alla prima banda specificata se il valore **Bandwidth Utilization (Utilizzo banda)** di quella banda è inferiore al valore impostato. Altrimenti il client verrà indirizzato alla seconda opzione specificata in **Target Band**.



## Rilevamento bounce

Questi controlli permettono di specificare quante volte un client può essere reindirizzato. Questo serve ad impedire che un client venga reindirizzato troppe volte. Tuttavia non previene la disconnessione dei client e non impedisce ai client di cambiare banda autonomamente. Ciascun client può essere reindirizzato N volte (**Counts**) all'interno della finestra temporale specificata **Window Time (Periodo finestra)**. Quando il limite è stato raggiunto il client non verrà più reindirizzato per il periodo specificato in **Dwell Time (Periodo di riposo)**.



## 5 Utility

---

### NOTE:

- Scaricate e installate le utility per il router wireless dal sito web ASUS:
  - Device Discovery v1.4.7.1 all'indirizzo <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Discovery.zip>
  - Firmware Restoration v1.9.0.4 all'indirizzo <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Rescue.zip>
  - Windows Printer Utility v1.0.5.5 all'indirizzo <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Printer.zip>
  - Queste utility non sono compatibili con Mac OS.
- 

### 5.1 Device Discovery

Device Discovery è un'utility ASUS WLAN che vi permette di localizzare il router wireless ASUS e configurarne le impostazioni della rete wireless.

#### **Per lanciare l'utility Device Discovery:**

- Dal Desktop di Windows® cliccate su **Start > All Programs (Tutti i programmi) > ASUS Utility > ASUS Wireless Router > Device Discovery.**

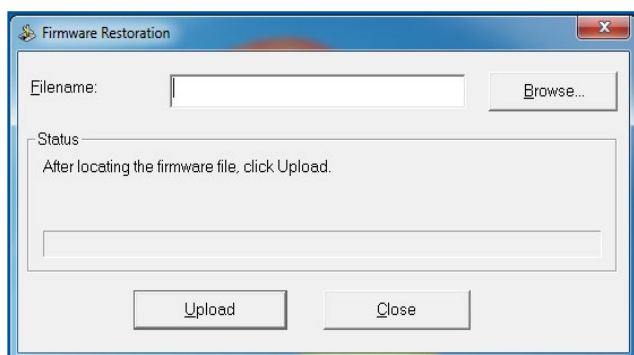
---

**NOTA:** Quando impostate il router in modalità Access Point avete bisogno di usare Device Discovery per ottenere l'indirizzo IP del router.

---

## 5.2 Firmware Restoration

Firmware Restoration si usa su un router wireless ASUS quando l'aggiornamento del firmware è fallito. Questo carica il firmware che voi stessi specificate. L'intero processo può durare dai tre ai quattro minuti.



---

**IMPORTANTE:** Lanciate la modalità di recupero prima di eseguire l'utility Firmware Restoration.

---

**NOTA:** Questa caratteristica non è supportata in Mac OS.

---

### Per lanciare la modalità di recupero e eseguire l'utility Firmware Restoration:

1. Scollegate il router dalla sorgente di alimentazione.
2. Tenete premuto il pulsante di reset che trovate sul pannello posteriore e, contemporaneamente, collegate il cavo di alimentazione. Rilasciate il pulsante di reset quando il LED di alimentazione sul pannello anteriore lampeggia lentamente. Questo indica che il router è in modalità di recupero.

3. Assegnate un indirizzo IP statico al vostro computer e usate le seguenti istruzioni per configurare le vostre impostazioni TCP/IP:

**Indirizzo IP:** 192.168.1.x

**Maschera di sottorete:** 255.255.255.0

4. Dal desktop cliccate su **Start > Tutti i programmi > ASUS Utility GT-AC29000 Wireless Router > Firmware Restoration.**
5. Selezionate il file specifico e poi cliccate su **Upload (Carica).**

---

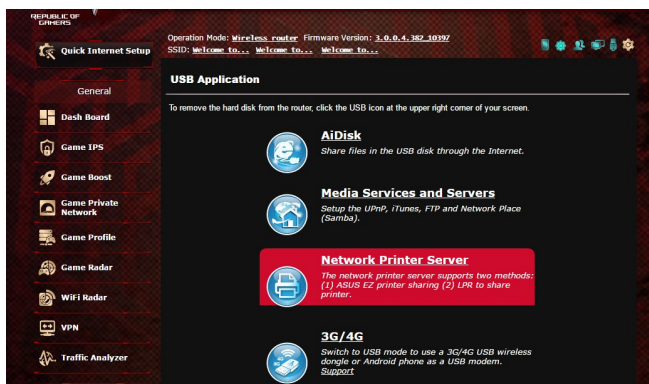
**NOTA:** Questo non è un programma per l'aggiornamento del firmware e non può essere utilizzato su un router wireless ASUS funzionante. I normali aggiornamenti del firmware devono essere fatti attraverso l'interfaccia web. Fate riferimento al *Capitolo 4: Impostazioni avanzate* per maggiori dettagli.

---

## 5.3 Impostare il server di stampa

### 5.3.1 ASUS EZ Printer Sharing

ASUS EZ Printer Sharing vi permette di connettere una stampante USB alla porta USB del vostro router wireless e creare un server di stampa. In questo modo i client della vostra rete possono stampare file o fare scansioni di documenti senza bisogno di cavi.



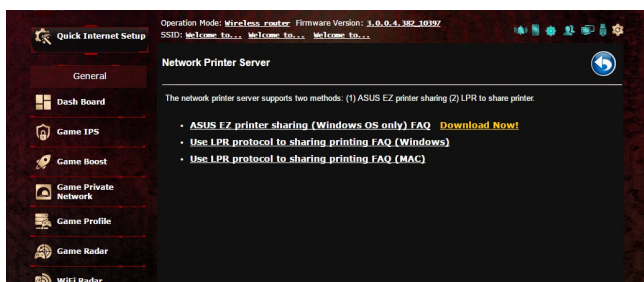
---

**NOTA:** Le funzioni del server di stampa sono supportate su Windows® 7/8/8.1/10.

---

## Per configurare la modalità condivisione stampante EZ:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate) > USB Application (Applicazioni USB) > Network Printer Server (Server di stampa di rete)**.
2. Cliccate su **Download Now (Scarica Adesso)** per scaricare l'utility per la stampante di rete.

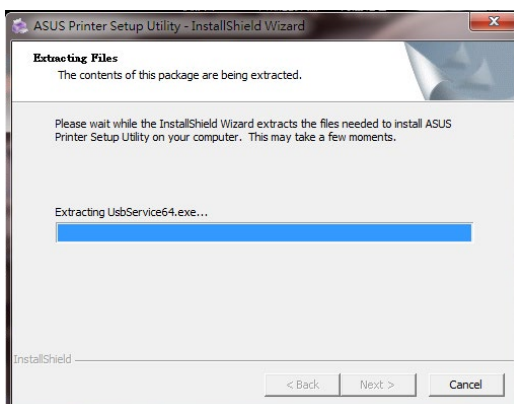
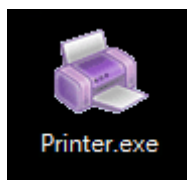


---

**NOTA:** L'utility per le stampanti di rete è supportata su Windows® 7/8/8.1/10. Per installare l'utility su Mac OS selezionate **Use LPR protocol for sharing printer (Usa il protocollo LPR per condividere la stampante)**.

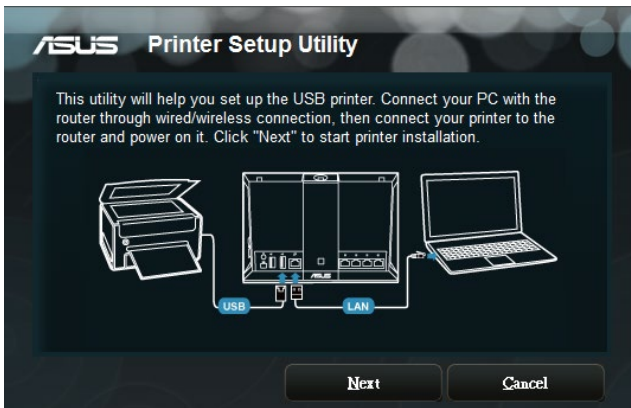
---

3. Estraiete il file dall'archivio e cliccate sull'icona della stampante per far partire il programma di installazione della stampante.





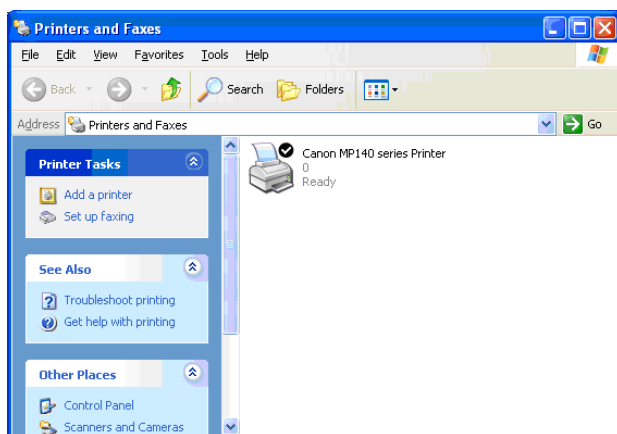
4. Seguite le istruzioni sullo schermo per completare il processo di installazione dell'hardware e poi cliccate su **Next (Avanti)**.



5. Attendete alcuni minuti sino al completamento del setup iniziale. Cliccate su **Next (Avanti)**.
6. Cliccate su **Finish (Fine)** per completare l'installazione.
7. Seguite le istruzioni di Windows per installare correttamente i driver della stampante.



8. Quando avrete installato correttamente i driver della stampante gli altri dispositivi di rete potranno cominciare ad usare la vostra stampante condivisa.



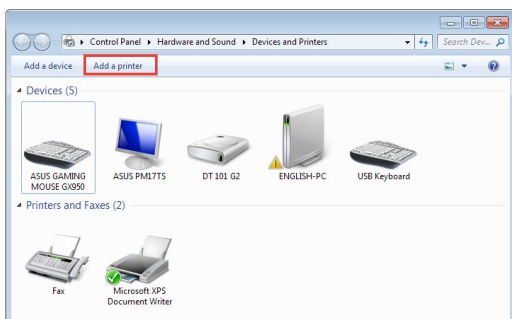
## 5.3.2 Utilizzo di LPR per condividere una stampante

Potete condividere una stampante con i vostri computer Windows® e MAC usando il protocollo LPR/LPD (Line Printer Remote/Line Printer Daemon).

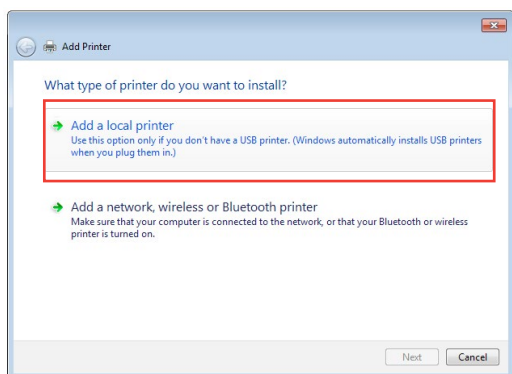
### Condividere la vostra stampante LPR

**Per condividere la vostra stampante LPR:**

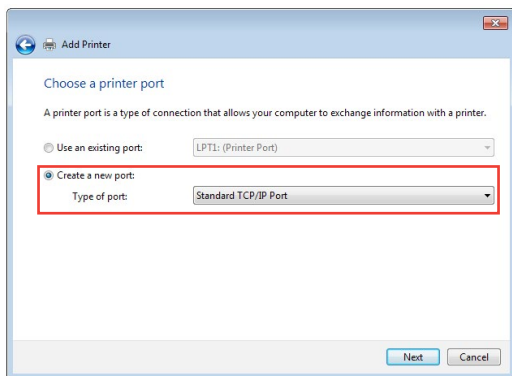
1. Dal Desktop di Windows® cliccate su **Start > Devices and Printers (Dispositivi e Stampanti) > Add a printer (Aggiungi stampante)** per far partire la procedura guidata **Add Printer Wizard (Aggiungi stampante)**.



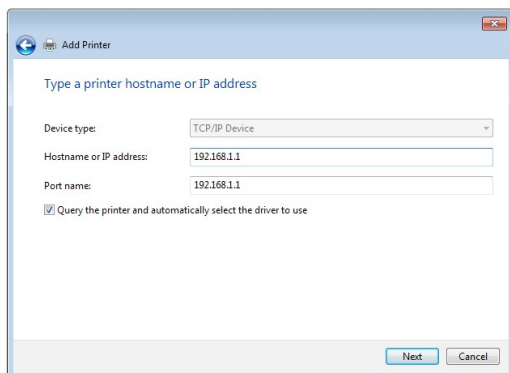
2. Selezionate **Add a local printer (Aggiungi stampante locale)** e poi cliccate su **Next (Avanti)**.



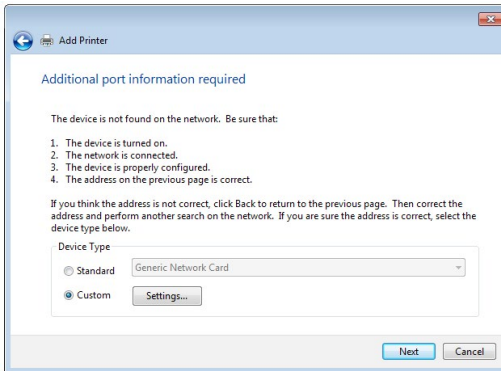
3. Selezionate **Create a new port (Crea una nuova porta)** e poi impostate il tipo **Standard TCP/IP Port** nel campo **Type of Port (Tipo di porta)**. Cliccate su **New Port (Avanti)**.



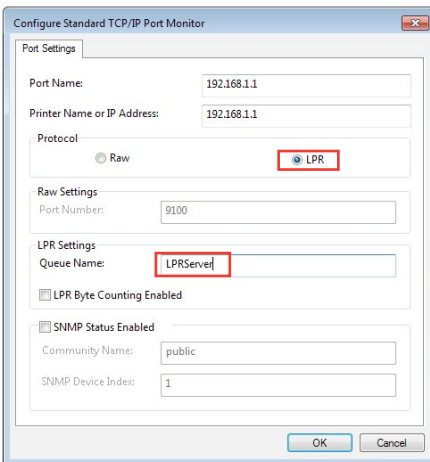
4. Nel campo **Hostname or IP address (Nome host o indirizzo IP)** inserite l'indirizzo IP del router wireless e poi cliccate su **Next (Avanti)**.



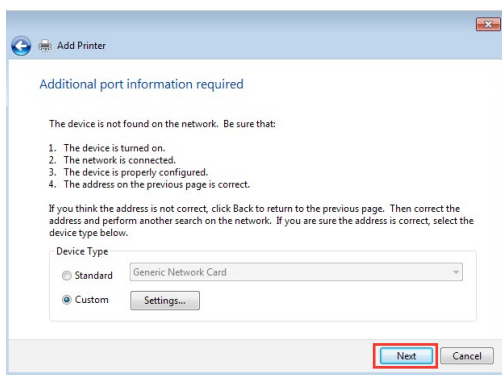
5. Selezionate **Custom (Personalizzata)** e poi cliccate su **Impostazioni**.



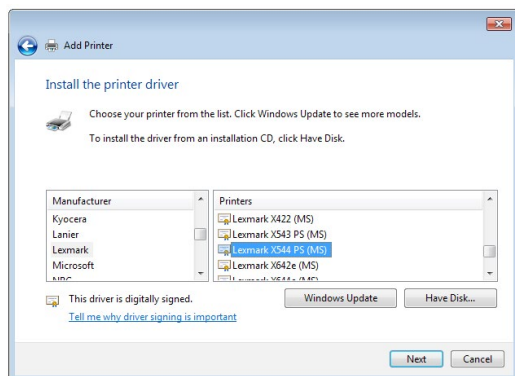
6. Impostate il **Protocol (Protocollo)** su **LPR**. Nel campo **Queue Name (Nome coda)** inserite **LPRServer** e poi cliccate su **OK** per continuare.



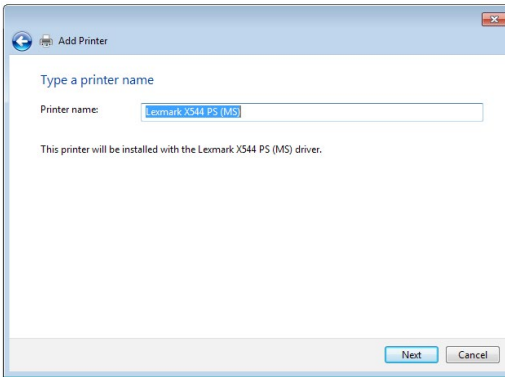
7. Cliccate su **Next (Avanti)** per completare le impostazioni della porta TCP/IP standard.



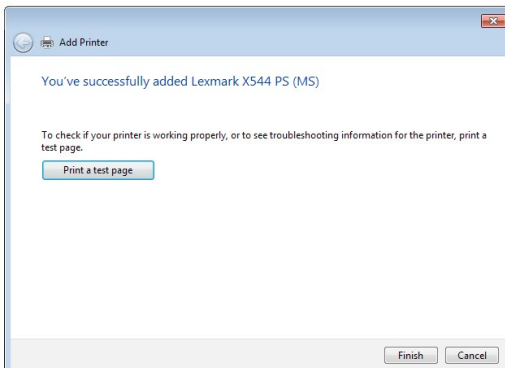
8. Installate i driver della stampante selezionando il produttore e il modello corretti dall'elenco. Se la vostra stampante non è nell'elenco cliccate su **Have Disk (Disco driver...)** per installare i driver da un supporto CD-ROM o da un file manualmente.



9. Cliccate su **Next (Avanti)** per accettare di usare il nome predefinito per la stampante.



10. Cliccate su **Finish (Fine)** per completare l'installazione.



## 5.4 Download Master

Download Master è un'applicazione che vi permette di scaricare file anche quando i vostri portatili, o altri dispositivi, sono spenti.

---

**NOTA:** Per utilizzare Download Master avete bisogno di un dispositivo di archiviazione USB connesso al router wireless.

---

### Per usare Download Master:

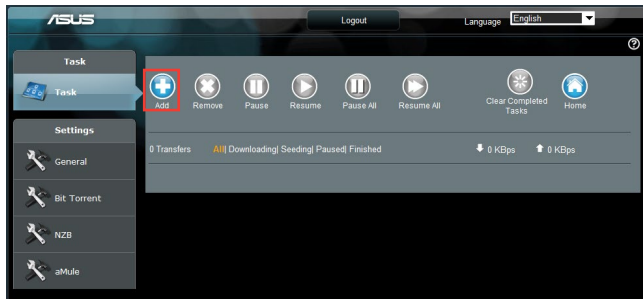
1. Cliccate su **Advanced Settings (Impostazioni avanzate)** > **USB application (Applicazioni USB)** > **Download Master** per scaricare e installare l'utility automaticamente.

---

**NOTA:** Se avete più di un dispositivo USB connesso al router selezionate il dispositivo USB che volete usare per il download dei file.

---

2. Quando il download è completato cliccate sull'icona di Download Master per iniziare ad usare l'applicazione.
3. Cliccate su **Add (Aggiungi)** per aggiungere un download.



4. Selezionate un protocollo di download come Torrent, HTTP o FTP. Se necessario fornite un file .torrent, o un magnet link, per iniziare il download.

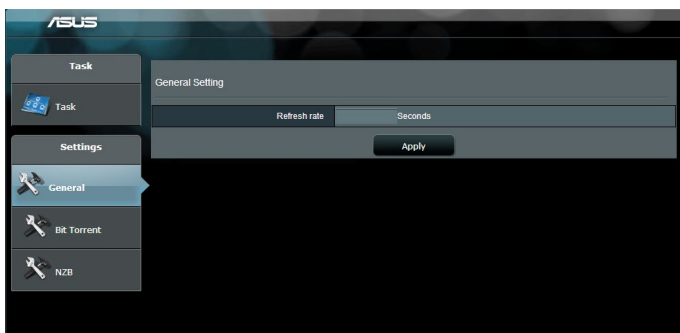
---

**NOTA:** Per maggiori dettagli fate riferimento alla sezione «5.4.1 Impostazioni Torrent».

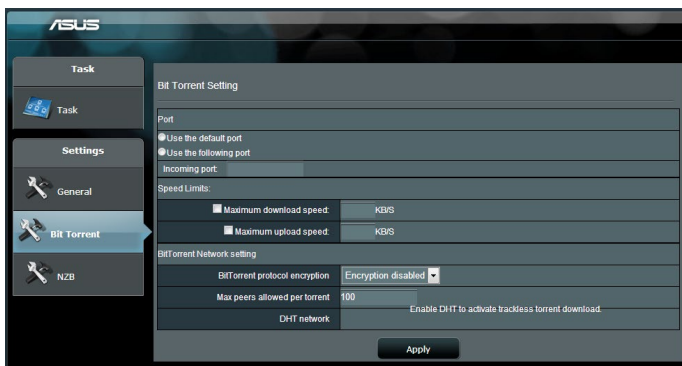
---



5. Usate il pannello di navigazione per le impostazioni avanzate.



## 5.4.1 Impostazioni Torrent

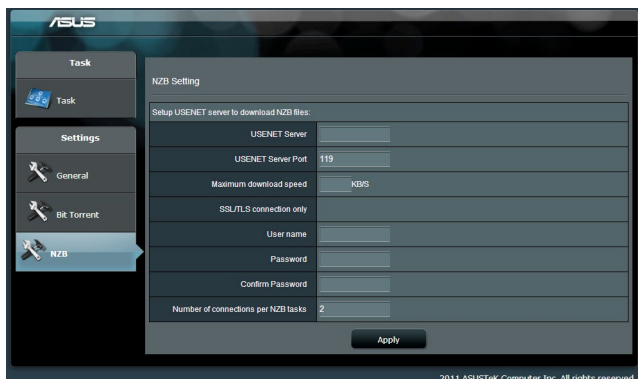


### Per configurare le impostazioni di download tramite Torrent:

1. Dalla pagina principale di Download Master cliccate su **Bit Torrent (Torrent)** per entrare nella pagina **BitTorrent Setting (Impostazioni Torrent)**.
2. Selezionate una porta specifica per i vostri download.
3. Per ridurre il rischio di congestione di rete potete impostare un valore massimo per la velocità di connessione in **Speed Limits (Limitazioni banda globale)**.
4. Potete anche limitare il numero massimo di connessioni simultanee e abilitare, o disabilitare, la cifratura dei file durante il download.

## 5.4.2 Impostazioni NZB

Avete la possibilità di configurare un server USENET per scaricare file .NZB. Dopo aver inserito le impostazioni per il server USENET cliccate su **Apply (Applica)**.



## 6 Risoluzione dei problemi

Questo capitolo fornisce soluzioni a vari problemi che potrebbero verificarsi durante il normale utilizzo del router. Se incontrate un problema che non è menzionato in questo capitolo visitate il sito di supporto ASUS al seguente indirizzo: <https://www.asus.com/it/support> per avere maggiori informazioni e per ottenere i contatti del supporto tecnico ASUS.

### 6.1 Risoluzione dei problemi più comuni

Se andate incontro a problemi con il vostro router provate a seguire questi semplici passi prima di cercare altre soluzioni.

#### Aggiornate il firmware all'ultima versione.

1. Aprite l'interfaccia web. Andate su **Advanced Settings (Impostazioni avanzate) > Administration (Amministrazione)** e scegliete la scheda **Firmware Upgrade (Aggiornamento firmware)**. Cliccate sul pulsante **Check (Controlla)** per verificare la presenza di aggiornamenti disponibili.
2. Se un nuovo firmware è disponibile visitate il sito: <https://www.asus.com/Networking/ROG-Rapture-GT-AC2900/HelpDesk/BIOS/> per ottenere il firmware aggiornato.
3. Dalla pagina **Firmware Upgrade (Aggiornamento firmware)** cliccate su **Choose File (Sfoglia)** per cercare il file del firmware che avete appena scaricato.
4. Cliccate su **Upload (Carica)** per aggiornare il firmware.

#### Riavvio della rete:

1. Spegnete il modem.
2. Scollegate il modem dalla rete.
3. Spegnete il router e i computer.
4. Collegate il modem.
5. Accendete il modem e aspettate 2 minuti.
6. Accendete il router e aspettate 2 minuti.
7. Accendete i computer.

## Controllate che tutti i cavi Ethernet siano collegati correttamente.

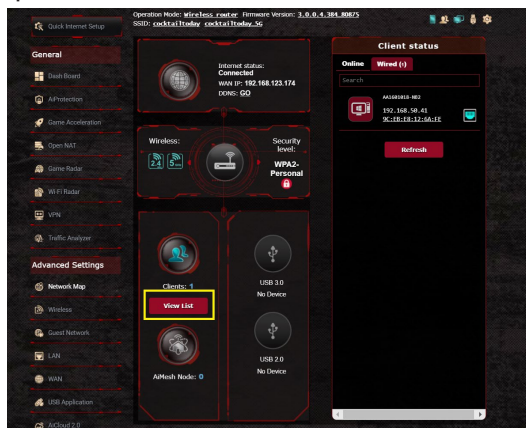
- Quando il cavo Ethernet che connette il router al modem è collegato correttamente il LED WAN sul router è acceso.
- Quando il cavo Ethernet che connette il vostro computer (acceso) al router è collegato correttamente il LED LAN corrispondente sul router è acceso.

## Controllate che le impostazioni wireless del vostro computer siano uguali a quelle del router.

- Quando collegate il vostro computer al router tramite rete wireless assicuratevi che il SSID, l'encryption method (metodo di cifratura) e la password siano corretti.

## Assicuratevi che le vostre impostazioni di rete siano corrette.

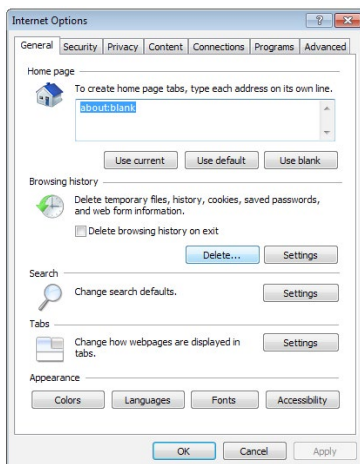
- Ogni client sulla rete deve avere un indirizzo IP valido. ASUS raccomanda di usare il server DHCP del router wireless per assegnare automaticamente gli indirizzi IP ai computer della vostra rete.
- Alcuni fornitori di connessione dati via cavo potrebbero richiedere che l'indirizzo MAC del vostro computer sia registrato con il vostro utente prima di permettere la connessione. Potete visualizzare il vostro indirizzo MAC dall'interfaccia web andando su **Network Map > Clients** e posizionando il puntatore sul vostro dispositivo nella sezione **Client Status (Stato client)**. L'indirizzo MAC è formato da 6 coppie di cifre esadecimali, con ciascuna coppia separata da un trattino, per un totale di 12 cifre. Ad esempio: 00-50-FC-A0-67-2C.



## 6.2 Domande frequenti (FAQ)

### Impossibile accedere all'interfaccia web usando il browser Internet

- Se il vostro computer è collegato via cavo controllate accuratamente la connessione del cavo e lo stato dei LED come descritto nelle sezioni precedenti.
- Assicuratevi di usare le corrette informazioni di login. Il nome utente e la password predefinite sono entrambe "admin". Assicuratevi che il tasto "BLOCCO MAIUSCOLE" sia disattivato quando inserite il nome utente e la password.
- Rimuovete i cookie e i file temporanei dal vostro browser. Per Internet Explorer 8 la procedura standard per rimuovere i cookie e i file temporanei è la seguente:
  1. Lanciate Internet Explorer 8 e cliccate su **Strumenti** > **Opzioni Internet**.
  2. Nella scheda **Generale**, nel riquadro **Cronologia esplorazioni** cliccate su **Elimina...**, selezionate le voci **File temporanei Internet** e **Cookie** e poi cliccate su **Elimina**.



---

#### NOTE:

- La procedura per la rimozione dei cookie e dei file temporanei potrebbe variare a seconda del browser utilizzato.
  - Disabilitate il server proxy, le connessioni remote e configurate le impostazioni TCP/IP in modo da ottenere un indirizzo IP automaticamente. Per maggiori informazioni fate riferimento al *Capitolo 1* di questo manuale.
  - Assicuratevi di usare cavi Ethernet CAT5 o CAT6.
-

## Il client non riesce a stabilire una connessione wireless con il router.

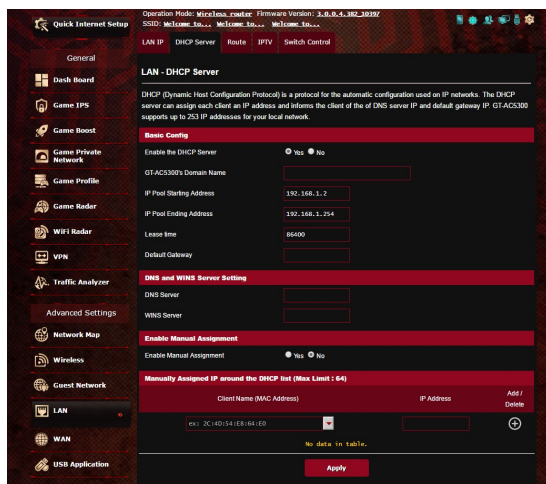
**NOTA:** Se riscontrate dei problemi nel connettervi alla rete wireless a 5Ghz assicuratevi che il vostro dispositivo wireless sia in grado di supportare i 5Ghz o le reti dual-band.

- **Fuori portata:**

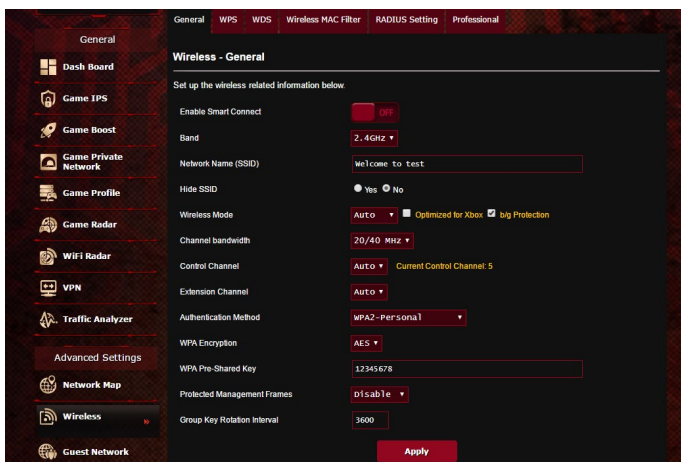
- Avvicinate il router al client wireless.
- Provate a modificare l'angolazione delle antenne del router per trovare la direzione migliore come descritto nella sezione «1.5 Posizionamento del router».

- **Il server DHCP è stato disabilitato:**

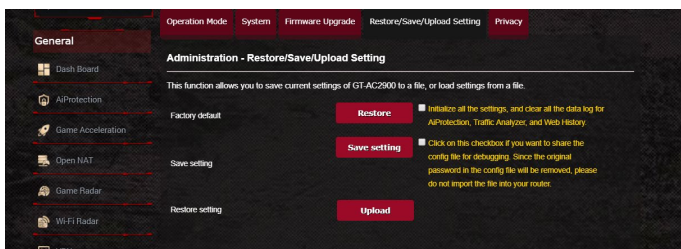
1. Aprite l'interfaccia web. Andate su **Advanced Settings (Impostazioni avanzate) > Network Map (Mappa di rete) > Clients (Client)** e cercate il dispositivo che volete connettere al router.
2. Se non riuscite a trovare il dispositivo nella **Network Map (Mappa di rete)** andate su **Advanced Settings (Impostazioni avanzate) > LAN > DHCP Server (Server DHCP)**, posizionatevi sul riquadro **Basic Config (Configurazione di base)** e selezionate **Yes (Sì)** all'opzione **Enable the DHCP Server (Abilita il server DHCP)**.



- Il nome della rete (SSID) non è visibile. Se il vostro dispositivo visualizza reti disponibili provenienti da altri router, ma non la rete del vostro router, andate su **Advanced Settings (Impostazioni avanzate) > Wireless > General (Generale)**, selezionate **No** alla voce **Hide SSID (Nascondi SSID)** e selezionate **Auto (Automatico)** alla voce **Control Channel (Canale di controllo)**.



- Se state usando un adattatore per la rete wireless assicuratevi che il canale che state usando sia conforme con i canali wireless disponibili nella vostra zona. Se così non fosse correggete il canale, la sua larghezza di banda e la modalità wireless.
- Se ancora non riuscite a connettervi al router in modalità wireless potete resettare il router alle impostazioni predefinite di fabbrica. Aprite l'interfaccia web, andate su **Administration (Amministrazione)**, selezionate la scheda **Restore/Save/Upload Setting (Impostazione Ripristina/Salva/Carica)** e cliccate sul pulsante **Restore (Ripristina)**.



## Nessun accesso a Internet.

- Verificate che il vostro router si possa connettere all'indirizzo IP pubblico (WAN) del vostro ISP. Per fare questo aprite l'interfaccia web e andate su **Advanced Settings (Impostazioni avanzate) > Network Map (Mappa di rete)** e controllate la voce **Internet Status (Stato Internet)**.
- Se il vostro router non riesce a raggiungere l'IP pubblico del vostro ISP provate a riavviare il router seguendo il procedimento consigliato nella sezione «Riavvio della rete» del paragrafo «Risoluzione dei problemi».



- Il dispositivo è stato bloccato tramite la funzione Parental Control (Controllo Genitori). Andate sulla scheda **General (Generale) > AiProtection Pro > Parental Controls (Controllo genitori)** e verificate se il dispositivo è presente nell'elenco. Se il dispositivo è nell'elenco **Client Name (Nome client)** rimuovete il dispositivo usando il pulsante **Delete (Elimina)** o modificate le impostazioni di **Time Management (Gestione tempo)**.
- Se ancora non avete accesso ad Internet provate a riavviare il computer e, in seguito, controllate il suo indirizzo IP di rete e l'indirizzo del gateway predefinito.
- Controllate lo stato degli indicatori presenti sul modem ADSL e sul router wireless. Se il LED WAN sul wireless router è spento controllate che tutti i cavi siano collegati correttamente.

## Avete dimenticato il nome della rete (SSID) o la password di protezione

- Impostate un nuovo SSID e una nuova chiave di protezione collegandovi al router tramite un cavo Ethernet. Aprite l'interfaccia web, andate su **Network Map (Mappa di rete)**, cliccate sull'icona del router, inserite un nuovo SSID e una nuova chiave di protezione e poi cliccate su **Apply (Applica)**.



- Ripristinate le impostazioni predefinite del router. Aprite l'interfaccia web, andate su **Administration (Amministrazione)**, selezionate la scheda **Restore/Save/Upload Setting (Impostazione Ripristina/Salva/Carica)** e cliccate sul pulsante **Restore (Ripristina)**. Il nome utente e la password predefinite sono entrambe "admin".

## Come faccio a ripristinare le impostazioni predefinite del router?

- Andate su **Administration (Amministrazione)**, selezionate la scheda **Restore/Save/Upload Setting (Impostazione Ripristina/Salva/Carica)** e cliccate sul pulsante **Restore (Ripristina)**.

Queste sono le impostazioni predefinite di fabbrica:

<b>Nome utente:</b>	admin
<b>Password:</b>	admin
<b>Abilita Server DHCP:</b>	Sì (se il cavo WAN è collegato)
<b>Indirizzo IP:</b>	http://router.asus.com (o 192.168.1.1)
<b>Nome dominio:</b>	(Vuoto)
<b>Maschera di sottorete:</b>	255.255.255.0
<b>Server DNS primario:</b>	192.168.1.1
<b>Server DNS secondario:</b>	(Vuoto)
<b>SSID (2.4GHz):</b>	ASUS
<b>SSID (5GHz):</b>	ASUS_5G

## Aggiornamento del firmware non riuscito.

Lanciate la modalità di recupero e eseguite l'utility Firmware Restoration. Fate riferimento alla sezione *5.2 Firmware Restoration* per avere maggiori informazioni su come effettuare il recupero del firmware.

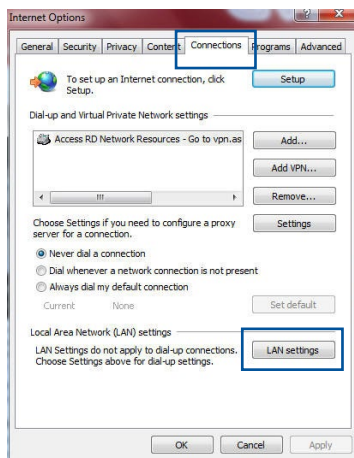
## Impossibile accedere all'interfaccia web

Prima di procedere con la configurazione del router portate a termine i seguenti passaggi sul vostro computer e su eventuali altri computer presenti nella vostra rete.

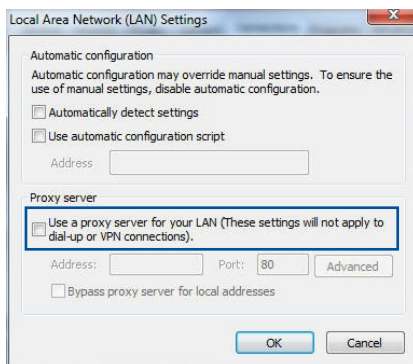
### A. Disabilitate il server proxy (se abilitato).

#### Windows® 7

1. Cliccate su **Start > Internet Explorer** per aprire il browser.
2. Cliccate su **Tools (Strumenti) > Internet options (Opzioni Internet)**, selezionate la scheda **Connections (Connessioni)** e cliccate su **LAN settings (Impostazioni LAN)**.

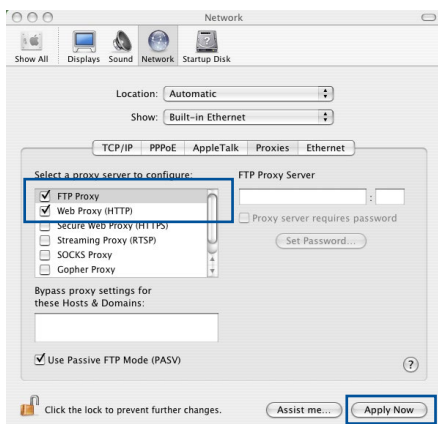


3. Dalla schermata di impostazioni della vostra LAN (Local Area Network) togliete la spunta da **Use a proxy server for your LAN (Utilizza un proxy server per le connessioni LAN)**.
4. Quando avete finito selezionate **OK**.



## MAC OS

1. Dal vostro browser Safari cliccate su **Safari > Preferences (Preferenze) > Advanced (Avanzate) > Change Settings (Modifica Impostazioni)**.
2. Dal pannello **Network** togliete la spunta da **FTP Proxy (Proxy FTP)** e **Web Proxy (HTTP) (Proxy web (HTTP))**.
3. Quando avete finito selezionate **Apply Now (Applica)**.

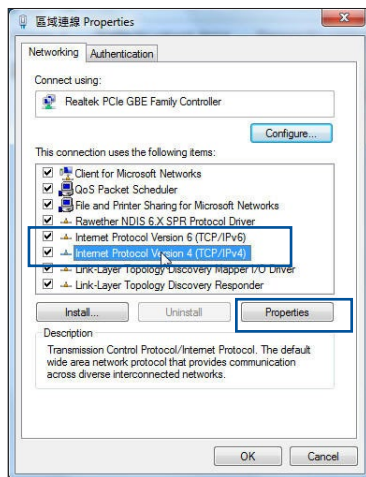


**NOTA:** Fate riferimento alla funzione *Aiuto* del vostro browser per dettagli su come disabilitare una connessione remota.

## B. Configurate le impostazioni TCP/IP in modo da ottenere un indirizzo IP automaticamente.

### Windows® 7

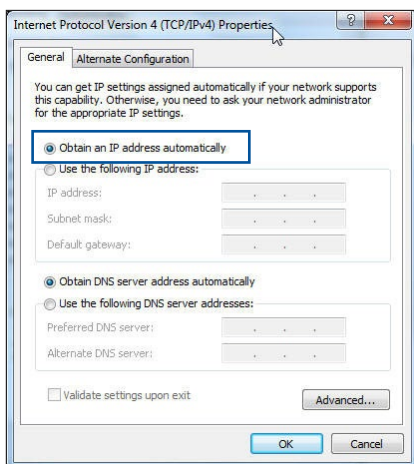
1. Cliccate su **Start > Control Panel (Pannello di controllo) > Network and Internet (Rete e Internet) > Manage network connections (Gestisci connessioni di rete)**.
2. Selezionate **Protocollo Internet versione 4 (TCP/IPv4)** o **Internet Protocol Version 6 (TCP/IPv6)** (Protocollo Internet versione 6 (TCP/IPv6)) e poi cliccate su **Proprietà**.




3. Per ottenere automaticamente le impostazioni IPv4 selezionate **Otteni automaticamente un indirizzo IP**.

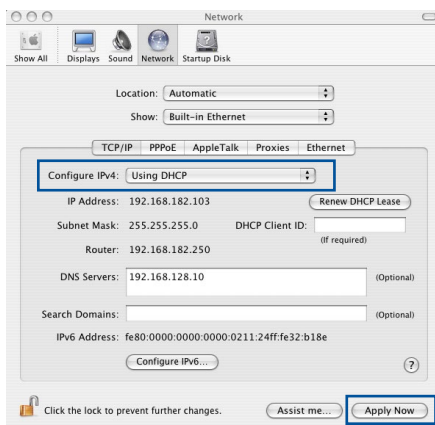
Per ottenere automaticamente le impostazioni IPv6 selezionate **Obtain an IPv6 address automatically (Ottieni automaticamente un indirizzo IPv6)**.

4. Quando avete finito selezionate **OK**.



## MAC OS

1. Cliccate sull'icona della mela  sulla parte in alto a destra del vostro schermo.
2. Cliccate su **System Preferences (Preferenze di Sistema) > Network (Rete) > Configure... (Configura...)**.
3. Dal pannello **TCP/IP** selezionate **Using DHCP (Utilizzo di DHCP)** nell'elenco **Configure IPv4 (Configura IPv4)**.
4. Quando avete finito selezionate **Apply Now (Applica)**.

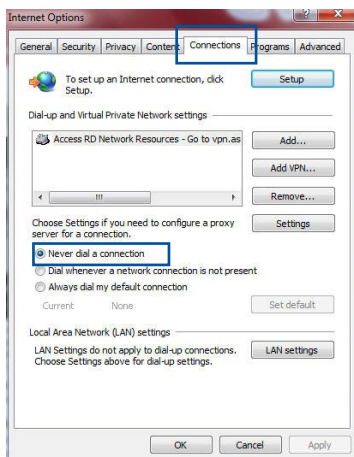


**NOTA:** Fate riferimento alle informazioni su aiuto e supporto del vostro sistema operativo per avere maggiori dettagli sulla configurazione delle impostazioni TCP/IP del vostro computer.

## C. Disabilitate la connessione remota (se abilitata).

### Windows® 7

1. Cliccate su **Start > Internet Explorer** per aprire il browser.
2. Cliccate su **Tools (Strumenti) > Internet options (Opzioni Internet)** e selezionate la scheda **Connections (Connessioni)**.
3. Selezionate la voce **Never dial a connection (Non utilizzare mai connessioni remote)**.
4. Quando avete finito selezionate **OK**.



---

**NOTA:** Fate riferimento alla sezione *Aiuto* del vostro browser per dettagli su come disabilitare una connessione remota.

---

# Appendice

## Comunicazioni

### Servizio di ritiro e riciclaggio ASUS

Il programma di ritiro e riciclaggio dei prodotti ASUS deriva dal costante impegno aziendale a raggiungere i più elevati standard di protezione ambientale. ASUS crede, infatti, di poter fornire soluzioni in grado di riciclare in modo responsabile non soltanto i prodotti, le batterie e le altre componenti elettroniche, ma anche i materiali utilizzati per l'imballaggio. Per informazioni dettagliate sulle modalità di riciclaggio nei vari paesi visitate la pagina: <http://csr.asus.com/english/Takeback.htm>.

### Comunicazione REACH

Nel rispetto del regolamento REACH (Registration, Evaluation, Authorization and Restriction of Chemicals) le sostanze chimiche contenute nei prodotti ASUS sono state pubblicate sul sito web ASUS REACH: <http://csr.asus.com/english/REACH.htm>

### Dichiarazione FCC (Federal Communications Commission)

Questo dispositivo rispetta i requisiti indicati nel regolamento FCC - Parte 15. Il funzionamento è soggetto alle seguenti due condizioni:

- Questo dispositivo non provoca interferenze dannose.
- Questo dispositivo accetta qualsiasi interferenza comprese quelle che potrebbero causare un comportamento indesiderato.

I collaudi ai quali è stato sottoposto questo apparecchio ne dimostrano la conformità ai limiti stabiliti per i dispositivi digitali di classe B, come indicato dal paragrafo 15 delle norme FCC. Questi limiti sono stati definiti per offrire una ragionevole protezione contro le interferenze dannose quando l'apparecchio viene usato in ambienti residenziali.

Questo apparecchio genera, usa e può emettere energia in radiofrequenza e, se non viene installato e utilizzato come indicato nel manuale d'uso, può provocare interferenze dannose alle comunicazioni radio. Non è tuttavia possibile garantire che non si verifichino interferenze in casi particolari. Se questo apparecchio causasse interferenze dannose alla ricezione di programmi radiofonici e televisivi, fatto verificabile spegnendo e riaccendendo l'apparecchio stesso, consigliamo all'utente di provare a correggere l'interferenza in uno o più dei seguenti modi:

- Riorientate o riposizionate l'antenna ricevente.
- Aumentate la distanza tra il dispositivo e il ricevitore.
- Collegate l'apparecchio ad una diversa presa di corrente in modo che apparecchio e ricevitore si trovino su circuiti diversi.
- Consultate, per richiedere assistenza, il rivenditore o un tecnico radio/TV qualificato.

---

**AVVERTIMENTO!** Eventuali modifiche o cambiamenti, non espressamente approvati dall'autorità responsabile per la conformità, potrebbero invalidare il diritto dell'utente all'utilizzo di questo apparecchio.

---

## Divieto di Co-ubicazione

Il dispositivo e la/le sua/e antenna/e non devono essere collocate insieme né funzionare in concomitanza con altre antenne o trasmettitori.

### AVVISO IMPORTANTE:

**Dichiarazione sull'esposizione a radiazioni:** Questo apparecchio è conforme ai limiti FCC, per l'esposizione a radiazioni, stabiliti per un ambiente non controllato. L'utente deve attenersi strettamente alle specifiche istruzioni operative in modo da soddisfare i requisiti richiesti in materia. Per un utilizzo conforme ai requisiti per l'esposizione FCC seguite le istruzioni operative come indicato in questo manuale.

---

**AVVERTIMENTO!** Questo dispositivo deve essere installato e utilizzato secondo le istruzioni fornite. L'antenna, o le antenne, usate per questo trasmettitore devono essere installate ad una distanza di almeno 20 cm dalle persone e non devono essere collocate o operare in concomitanza di qualsiasi altra antenna o trasmettente.

---

## Comunicazioni sulla sicurezza

- Usate questo prodotto in ambienti la cui temperatura sia compresa tra 0°C(32°F) e 40°C(104°F).
- Consultate l'etichetta indicante la potenza posta sul fondo del prodotto e assicuratevi che il vostro adattatore di alimentazione sia compatibile con tali valori.
- Non collocate il dispositivo su superfici irregolari o instabili. Contattate il servizio clienti se lo chassis è stato danneggiato.
- NON riponete oggetti sopra e non infilate alcun oggetto all'interno del prodotto.
- NON esponete a liquidi, pioggia o umidità. NON usate il modem durante i temporali.
- NON coprite le prese d'aria del prodotto per evitare che il sistema si surriscaldi.
- NON utilizzate cavi di alimentazione, accessori o periferiche danneggiate.
- Se l'adattatore è danneggiato non provate a ripararlo da soli. Contattate un tecnico qualificato o il vostro rivenditore.
- Per prevenire il rischio di scosse elettriche scollegate il cavo di alimentazione dalla presa di corrente prima di spostare il sistema.

## Comunicazioni sulla sicurezza

- Utilisez ce produit dans un environnement dont la température ambiante est comprise entre 0°C (32°F) et 40°C (104°F).
- Référez-vous à l'étiquette située au dessous du produit pour vérifier que l'adaptateur secteur répond aux exigences de tension.
- NE PAS placer sur une surface irrégulière ou instable. Contactez le service après-vente si le châssis a été endommagé.
- NE PAS placer, faire tomber ou insérer d'objets sur/dans le produit.
- NE PAS exposer l'appareil à la pluie ou à l'humidité, tenez-le à distance des liquides. NE PAS utiliser le modem lors d'un orage.
- NE PAS bloquer les ouvertures destinées à la ventilation du système pour éviter que celui-ci ne surchauffe.

- NE PAS utiliser de cordons d'alimentation, d'accessori ou autres périphériques endommagés.
- Si l'adaptateur est endommagé, n'essayez pas de le réparer vous-même. Contactez un technicien électrique qualifié ou votre revendeur.
- Pour éviter tout risque de choc électrique, débranchez le câble d'alimentation de la prise électrique avant de toucher au système.

## Dichiarazione sull'esposizione a radiazioni:

### Déclaration d'exposition aux radiations

Questo apparecchio è conforme ai limiti IC, per l'esposizione a radiazioni, stabiliti per un ambiente non controllato. Questo apparecchio deve essere installato e utilizzato ad una distanza di almeno 31 cm dal corpo.

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 31 cm de distance entre la source de rayonnement et votre corps.

Questo dispositivo contiene trasmettitori/ricevitori esenti da licenza e compatibili con gli RSS di Innovation, Science and Economic Development Canada. Il funzionamento è soggetto alle seguenti due condizioni:

- (1) Questo dispositivo non provoca interferenze dannose.
- (2) Questo apparecchio accetta qualsiasi interferenza comprese quelle che potrebbero causare un comportamento indesiderato.

*Cet appareil contient des émetteurs / récepteurs exempts de licence qui sont conformes au (x) RSS (s) exemptés de licence d'Innovation, Sciences et Développement économique Canada. L'opération est soumise aux deux conditions suivantes:*

- (1) Cet appareil ne doit pas provoquer d'interférences.*
- (2) Cet appareil doit accepter toute interférence, y compris les interférences susceptibles de provoquer un fonctionnement indésirable de l'appareil.*

Questo trasmettitore radio [IC: 3568A-RTHR00] è stato approvato da Innovation, Science and Economic Development Canada per operare con le tipologie di antenna elencate qui di seguito e con il massimo guadagno possibile indicato. Le tipologie di antenne non indicate in questo elenco, aventi un guadagno superiore al massimo guadagno indicato per il tipo specifico, sono proibite per l'uso con questo dispositivo.

*Le présent émetteur radio (IC: 3568A-RTHR00) a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal d'antenne. Les types d'antennes non inclus dans cette liste qui ont un gain supérieur au gain maximal indiqué pour tout type listé sont strictement interdits pour une utilisation avec cet appareil.*



Set	Ant.	Porta				Marca	P/N	Tipo	Connettore	Guadagno (dBi)			
		2.4 GHz	5GHz B1/B2	5GHz B3	5GHz B4					2.4 GHz	5GHz B1/B2	5GHz B3	5GHz B4
1	1	1	-	4	4	WHA YU	C660-510413-A	Dipolo	Connettore SMA inverso	1.9	-	2.3	1.9
	2	2	-	3	3	WHA YU	C660-510413-A	Dipolo	Connettore SMA inverso	1.9	-	2.3	1.9
	3	3	-	2	2	WHA YU	C660-510413-A	Dipolo	Connettore SMA inverso	1.9	-	2.3	1.9
	4	4	-	1	1	WHA YU	C660-510413-A	Dipolo	Connettore SMA inverso	1.9	-	2.3	1.9
	5	-	1	-	-	WHA YU	C660-510413-A	Dipolo	Connettore SMA inverso	-	2.3	-	-
	6	-	2	-	-	WHA YU	C660-510413-A	Dipolo	Connettore SMA inverso	-	2.3	-	-
	7	-	3	-	-	WHA YU	C660-510413-A	Dipolo	Connettore SMA inverso	-	2.3	-	-
	8	-	4	-	-	WHA YU	C660-510413-A	Dipolo	Connettore SMA inverso	-	2.3	-	-
2	1	1	-	4	4	WHA YU	C660-510431-A	Dipolo	Connettore SMA inverso	1.9	-	2.3	1.9
	2	2	-	3	3	WHA YU	C660-510431-A	Dipolo	Connettore SMA inverso	1.9	-	2.3	1.9
	3	3	-	2	2	WHA YU	C660-510431-A	Dipolo	Connettore SMA inverso	1.9	-	2.3	1.9
	4	4	-	1	1	WHA YU	C660-510431-A	Dipolo	Connettore SMA inverso	1.9	-	2.3	1.9
	5	-	1	-	-	WHA YU	C660-510431-A	Dipolo	Connettore SMA inverso	-	2.3	-	-
	6	-	2	-	-	WHA YU	C660-510431-A	Dipolo	Connettore SMA inverso	-	2.3	-	-
	7	-	3	-	-	WHA YU	C660-510431-A	Dipolo	Connettore SMA inverso	-	2.3	-	-
	8	-	4	-	-	WHA YU	C660-510431-A	Dipolo	Connettore SMA inverso	-	2.3	-	-
3	1	1	-	4	4	PSA	RFDPA161000 SBLB801	Dipolo	Connettore SMA inverso	1.9	-	2.3	1.9
	2	2	-		3	PSA	RFDPA161000 SBLB801	Dipolo	Connettore SMA inverso	1.9	-	2.3	1.9
	3	3	-	2	2	PSA	RFDPA161000 SBLB801	Dipolo	Connettore SMA inverso	1.9	-	2.3	1.9
	4	4	-	1	1	PSA	RFDPA161000 SBLB801	Dipolo	Connettore SMA inverso	1.9	-	2.3	1.9
	5	-	1	-	-	PSA	RFDPA161000 SBLB801	Dipolo	Connettore SMA inverso	-	2.3	-	-
	6	-	2	-	-	PSA	RFDPA161000 SBLB801	Dipolo	Connettore SMA inverso	-	2.3	-	-
	7	-	3	-	-	PSA	RFDPA161000 SBLB801	Dipolo	Connettore SMA inverso	-	2.3	-	-
	8	-	4	-	-	PSA	RFDPA161000 SBLB801	Dipolo	Connettore SMA inverso	-	2.3	-	-

Selezione Dinamica della Frequenza (DFS) per i dispositivi operanti nelle bande 5250- 5350 MHz, 5470-5600 MHz e 5650-5725 MHz.

*Sélection dynamique de fréquences (DFS) pour les dispositifs fonctionnant dans les bandes 5250-5350 MHz, 5470-5600 MHz et 5650-5725 MHz.*

Per la banda 5150-5250 MHz è permesso l'uso del dispositivo solamente all'interno per ridurre potenziali interferenze dannose ai sistemi satellitari a canale mobile che usino lo stesso canale.

*les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.*

Il massimo guadagno permesso per l'antenna per i dispositivi operanti nelle bande 5250-5350 MHz e 5470-5725 MHz deve essere tale per cui il dispositivo sia comunque conforme ai limiti EIRP.

*le gain maximal d'antenne permis pour les dispositifs utilisant les bandes 5250-5350 MHz et 5470-5725 MHz doit se conformer à la limite de p.i.r.e.*

Il massimo guadagno permesso per l'antenna per i dispositivi operanti nella banda 5725-5850 MHz deve essere tale per cui il dispositivo sia comunque conforme ai limiti EIRP per le operazioni punto-punto e non punto-punto.

*le gain maximal d'antenne permis (pour les dispositifs utilisant la bande 5725-5850 MHz) doit se conformer à la limite de p.i.r.e. spécifiée pour l'exploitation point à point et non point à point, selon le cas.*

Solo per l'uso all'interno.

*Pour une utilisation en intérieur uniquement.*

## **AVVISO IMPORTANTE:**

### **Dichiarazione per l'esposizione a radiazioni IC (Canada)**

Questo apparecchio è conforme ai limiti per l'esposizione a radiazioni IC RSS-102 stabiliti per un ambiente non controllato. Questo apparecchio deve essere installato e utilizzato ad una distanza di almeno 31 cm dal corpo.

*Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 31 cm de distance entre la source de rayonnement et votre corps.*

## **Precauzioni per l'utilizzo del dispositivo**

- a. Prestate particolare attenzione alla sicurezza personale quando usate questo dispositivo in aeroporti, ospedali, stazioni di servizio e garage professionali.
- b. Interferenze con i dispositivi medici: mantenete una distanza di almeno 15 cm (6 pollici) tra i dispositivi medici impiantati e i prodotti ASUS per ridurre al massimo il rischio di interferenze.
- c. Utilizzate i prodotti ASUS in condizioni di buona ricezione per minimizzare il livello di radiazioni.
- d. Tenete il dispositivo lontano da donne incinte e dal basso ventre degli adolescenti.

## **Précautions d'emploi de l'appareil**

- a. Soyez particulièrement vigilant quant à votre sécurité lors de l'utilisation de cet appareil dans certains lieux (les avions, les aéroports, les hôpitaux, les stations-service et les garages professionnels).
- b. Évitez d'utiliser cet appareil à proximité de dispositifs médicaux implantés. Si vous portez un implant électronique (stimulateurs cardiaques, pompes à insuline, neurostimulateurs...), veuillez impérativement respecter une distance minimale de 15 centimètres entre cet appareil et votre corps pour réduire les risques d'interférence.
- c. Utilisez cet appareil dans de bonnes conditions de réception pour minimiser le niveau de rayonnement. Ce n'est pas toujours le cas dans certaines zones ou situations, notamment dans les parkings souterrains, dans les ascenseurs, en train ou en voiture ou tout simplement dans un secteur mal couvert par le réseau.
- d. Tenez cet appareil à distance des femmes enceintes et du bas-ventre des adolescents.



**AEEE Yönetmeliğine Uygundur. IEEE Yönetmeliğine Uygundur.**

- Bu Cihaz Türkiye analog şebekelerde çalışabilecek şekilde tasarlanmıştır.
- Cihazın ayrıntılı kurulum rehberi kutu içeriğinden çıkan CD içerisinde dir. Cihazın kullanıcı arayüzü Türkçe'dir.
- Cihazın kullanılması planlanan ülkelerde herhangi bir kısıtlaması yoktur. Ülkeler simgeler halinde kutu üzerinde belirtilmiştir.



<b>Produttore:</b>	<b>ASUSTeK Computer Inc.</b> Tel: +886-2-2894-3447 Indirizzo: 4F, No. 150, LI-TE RD., PEITOU, TAIPEI 112, TAIWAN
<b>Rappresentante autorizzato in Europa:</b>	<b>ASUS Computer GmbH</b> Indirizzo: HARKORT STR. 21-23, 40880 RATINGEN, GERMANY
<b>Distributori autorizzati in Turchia:</b>	<b>BOGAZICI BILGISAYAR TICARET VE SANAYI A.S.</b> <b>Tel./FAX N.:</b> +90 212 331 10 00 / +90 212 332 28 90 <b>Indirizzo:</b> ESENTEPE MAH. BUYUKDERE CAD. ERCAN HAN B BLOK NO.121 SISLI, ISTANBUL 34394 <b>CIZGI Elektronik San. Tic. Ltd. Sti.</b> <b>Tel./FAX N.:</b> +90 212 356 70 70 / +90 212 356 70 69 <b>Indirizzo:</b> GURSEL MAH. AKMAN SK.47B 1 KAGITHANE/ ISTANBUL <b>KOYUNCU ELEKTRONİK BİLGİ İŞLEM SİST. SAN. VE DİŞ TIC. A.S.</b> <b>Tel. N.:</b> +90 216 5288888 <b>Indirizzo:</b> EMEK MAH.ORDU CAD. NO:18, SARIGAZI, SANCAKTEPE ISTANBUL <b>ENDEKS BİLİŞİM SAN VE DİŞ TIC LTD ŞTİ</b> <b>Tel./FAX N.:</b> +90 216 523 35 70 / +90 216 523 35 71 <b>Indirizzo:</b> NECİP FAZİL BULVARI, KEYAP CARSI SITESİ, G1 BLOK, NO:115 Y.DUDULLU, UMRANIYE, ISTANBUL <b>PENTA TEKNOLOJİ URUNLERİ DAGITIM TICARET A.S</b> <b>Tel./FAX N.:</b> +90 216 528 0000 <b>Indirizzo:</b> ORGANİZE SANAYİ BOLGESİ NATO YOLU 4.CADDE NO:1 UMRANIYE, ISTANBUL 34775

# Contatti ASUS

## ASUSTeK COMPUTER INC.

Indirizzo 4F, No. 150, Li-Te Rd., Peitou, Taipei 112, Taiwan  
Telefono +886-2-2894-3447  
Fax +886-2-2890-7798  
Sito Web [www.asus.com](http://www.asus.com)

### Supporto Tecnico

Telefono +86-21-3842-9911  
Fax +86-21-5866-8722, est. 9101#  
Supporto Online <http://qr.asus.com/techserv>

## ASUS COMPUTER INTERNATIONAL (America)

Indirizzo 48720 Kato Rd., Fremont, CA 94538, USA  
Telefono +1-510-739-3777  
Fax +1-510-608-4555  
Sito Web <http://www.asus.com/us/>

### Supporto Tecnico

Telefono +1-812-282-2787  
Fax di Supporto +1-812-284-0883  
Supporto Online <http://qr.asus.com/techserv>

## ASUSTeK ITALY S.r.l. (Italia)

Indirizzo Strada Statale Padana Superiore, 28  
20063 Cernusco sul Naviglio (MI)

### Supporto Tecnico

Telefono/Notebook/Eee 199 400 089\*  
Altri Prodotti 199 400 059\*  
Sito Web [www.asus.it](http://www.asus.it)  
Supporto Online <http://qr.asus.com/techserv>

\*\*Per le chiamate da rete fissa Telecom Italia il costo della chiamata è di 0,12 euro al minuto iva inclusa. La durata massima della telefonata non può essere superiore a 120 minuti. Per le chiamate da cellulare il costo varia in base all'operatore utilizzato.

<b>Produttore:</b>	<b>ASUSTeK Computer Inc.</b>	
	Tel:	+886-2-2894-3447
	Indirizzo:	4F, No. 150, LI-TE RD., PEITOU, TAIPEI 112, TAIWAN
<b>Rappresentante autorizzato in Europa:</b>	<b>ASUS Computer GmbH</b>	
	Indirizzo:	HARKORT STR. 21-23, 40880 RATINGEN, GERMANY

## Dichiarazione di conformità CE

### Dichiarazione di conformità UE semplificata

ASUSTek Computer Inc. con la presente dichiara che questo dispositivo è conforme ai requisiti essenziali e alle altre disposizioni pertinenti con la direttiva 2014/53/EU. Il testo completo della dichiarazione di conformità UE è disponibile all'indirizzo [https://www.asus.com/Networking/ROG-Rapture-GT-AC2900/HelpDesk\\_Declaration/](https://www.asus.com/Networking/ROG-Rapture-GT-AC2900/HelpDesk_Declaration/).

### Dichiarazione di conformità con la direttiva Ecodesign 2009/125/EC

I test per i requisiti eco-design (EC) N. 1275/2008 e (EU) N. 801/2013 sono stati eseguiti. Quando il dispositivo si trova nella modalità Standby di rete le sue interfacce di rete e I/O sono in sospensione e potrebbero non funzionare correttamente. Per riattivare il dispositivo premete uno tra i pulsanti Wi-Fi on/off, LED on/off, reset o WPS.

Questo apparecchio è conforme ai limiti UE, per l'esposizione a radiazioni, stabiliti per un ambiente non controllato. Questo apparecchio deve essere installato e utilizzato ad una distanza di almeno 20 cm dal corpo.

Tutte le modalità operative:

2.4GHz: 802.11b, 802.11g, 802.11n (HT20), 802.11n (HT40), 802.11ac (VHT20), 802.11ac (VHT40)

5GHz: 802.11a, 802.11n (HT20), 802.11n (HT40), 802.11ac (VHT20), 802.11ac (VHT40), 802.11ac (VHT80)

I valori di frequenza, modalità e massima potenza di trasmissione per l'UE sono elencati di seguito:

2412-2472MHz (802.11g 6Mbps): 19.81 dBm


5180-5240MHz (802.11ac VHT20 MCS0): 20.1 dBm

5260-5320MHz (802.11ac VHT40 MCS0): 21.31 dBm

5500-5700MHz (802.11ac VHT80 MCS0): 27.48 dBm

L'utilizzo di questo dispositivo è limitato agli ambienti interni quando si sta utilizzando la banda di frequenze compresa tra i 5150 e i 5350 MHz.

L'adattatore deve essere installato vicino al dispositivo e facilmente accessibile.

	AT	BE	BG	CZ	DK	EE	FR
	DE	IS	IE	IT	EL	ES	CY
	LV	LI	LT	LU	HU	MT	NL
	NO	PL	PT	RO	SI	SK	TR
	FI	SE	CH	UK	HR		

## Comunicazioni sulla sicurezza

- Usa questo prodotto in ambienti la cui temperatura sia compresa tra 0°C(32°F) e 40°C(104°F).
- Consulta l'etichetta indicante la potenza posta sul fondo del prodotto e assicurati che l'adattatore di alimentazione sia compatibile con tali valori.
- Non collocare il dispositivo su superfici irregolari o instabili. Contatta il servizio clienti se lo chassis è stato danneggiato.
- NON riporre oggetti sopra il dispositivo e non infilare alcun oggetto all'interno del dispositivo.
- NON esporre a liquidi, pioggia o umidità. NON usare il modem durante i temporali.
- NON coprire le prese d'aria del prodotto per evitare che il sistema si surriscaldi.
- NON utilizzare cavi di alimentazione, accessori o periferiche danneggiate.
- Se l'adattatore è danneggiato non provare a ripararlo. Contatta un tecnico qualificato o il rivenditore.
- Per prevenire il rischio di scosse elettriche scollega il cavo di alimentazione dalla presa di corrente prima di spostare il sistema.
- NON montare questo dispositivo ad un'altezza superiore a 2 metri.