I23335

REPUBLIC OF GAMERS

# USER MANUAL

RAPTURE GT-BE98

Router da gioco a Banda quadrupla BE25000

ASUS

I23335
Prima edizione
Febbraio 2024



**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) nonchè 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 prodottesi 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 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, 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

# Indice

# Indice

# Indice

# 1 Conoscete il vostro router wireless

## 1.1 Benvenuti!

Vi ringraziamo per aver acquistato il router wireless ROG Rapture.

Questo router wireless, molto sottile ed elegante, è dotato di quadrupla bande wireless (2.4GHz x 1, 5GHz x2, 6GHz x 1), 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%.

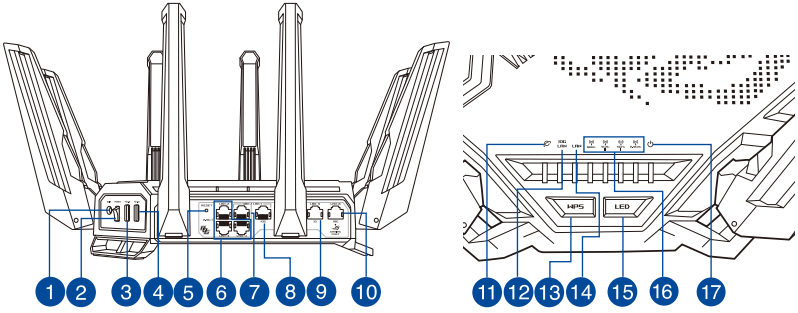
## 1.2 Contenuto della confezione

- ☑ Router gaming ROG Rapture
- ☑ Adattatore AC
- ☑ Cavo di rete Ethernet (RJ-45)
- ☑ Guida rapida

**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 Il vostro router wireless




| | |
|---|---|
| 1 | **Porta ingresso alimentazione (DCIN)**<br>Inserite l'alimentatore in dotazione in questo ingresso e collegate il router ad una sorgente di alimentazione. |
| 2 | **Interruttore di alimentazione**<br>Premere questo interruttore per accendere o spegnere il sistema. |
| 3 | **Porta USB 2.0**<br>Inserire un dispositivo compatibile con USB 2.0, come un disco rigido USB o una chiavetta USB, in questa porta. |
| 4 | **Porta USB 3.2 Gen 1**<br>Inserire un dispositivo compatibile con USB 3.2 Gen 1, come un disco rigido USB o una chiavetta USB, in questa porta. |
| 5 | **Pulsante di reset**<br>Questo pulsante serve a ripristinare le impostazioni predefinite di fabbrica. |
| 6 | **Porta LAN2-4 2.5GE**<br>Collegate i cavi di rete in queste porte per stabilire connessioni LAN 2.5GE. |
| 7 | **Porta WAN/LAN1 2.5GE**<br>Collegate un cavo di rete in questa porta per stabilire una connessione WAN / LAN1 2.5GE. |
| 8 | **Porta WAN/LAN1 10GE**<br>Collegate un cavo di rete in questa porta per stabilire una connessione WAN / LAN1 10GE. |
| 9 | **Porta LAN5 1GE**<br>Collegate un cavo di rete in questa porta per stabilire una connessione LAN5 1GE. |
| 10 | **Porta LAN6 10GE**<br>Collegate i cavi di rete in queste porte per avere priorità elevata. |
| 11 | **LED Internet (WAN) 10 / 2.5GE**<br>**Rosso:** Nessun indirizzo IP o nessuna connessione fisica.<br>**Acceso:** Connessione fisica alla rete Internet (WAN). |

| | |
|---|---|
| 12 | **LED LAN 10GE**<br>**Spento:** Nessuna alimentazione o nessuna connessione fisica.<br>**Acceso:** Connessione fisica alla rete locale (LAN) 10GE. |
| 13 | **Pulsante WPS**<br>Questo pulsante attiva la configurazione guidata di WPS. |
| 14 | **LED LAN**<br>**Spento:** Nessuna alimentazione o nessuna connessione fisica.<br>**Acceso:** Connessione fisica alla rete locale (LAN). |
| 15 | **Pulsante LED**<br>Premere questo pulsante per accendere/spegnere il LED. |
| 16 | **LED Wi-Fi 6GHz / 5GHz-2 / 5GHz-1 / 2.4GHz**<br>**Spento:** Nessun segnale 6GHz / 5GHz-2 / 5GHz-1 / 2.4GHz.<br>**Acceso:** Il sistema wireless è pronto.<br>**Lampeggiante:** Trasmissione o ricezione di dati tramite connessione wireless. |
| 17 | **LED alimentazione**<br>**Spento:** Nessuna alimentazione.<br>**Acceso:** Il dispositivo è pronto.<br>**Lampeggiante lentamente:** Modalità di recupero. |

**NOTE:**

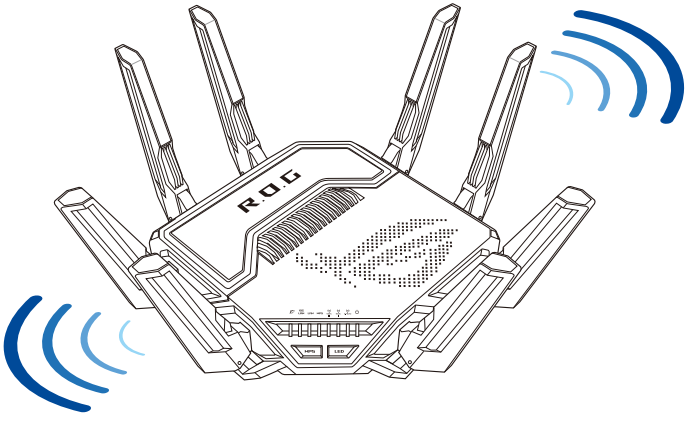
- Usate solamente l'adattatore di alimentazione che trovate nella confezione. L'utilizzo di altri adattatori potrebbe danneggiare il dispositivo.
- **Specifiche:**

| | | | |
|---|---|---|---|
| **Adattatore di alimentazione DC** | Uscita alimentatore DC: +19,5V con corrente massima 3,33A | | |
| **Temperatura di esercizio** | 0~40°C | Archiviazione | 0~70°C |
| **Umidità di esercizio** | 50~90% | Archiviazione | 20~90% |

## 1.4 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.
- Per assicurarvi la migliore qualità del segnale wireless orientare le otto antenne non rimovibili come mostrato nel disegno di seguito.



## 1.5 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/1000BaseTX)
- Connettività wireless IEEE 802.11a/b/g/n/ac/ax/be
- 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 802.11a/b/g/n/ac/ax/be, per connettervi alla rete wireless.
- Grazie alla tecnologia quadrupla band il vostro router wireless supporta simultaneamente i segnali wireless 2.4Ghz, 5GHz e 6GHz. 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 le bande a 5Ghz e 6GHz.
- Alcuni dispositivi IEEE 802.11n che volete connettere alla rete potrebbero non essere compatibili con lo standard a 5Ghz e 6GHz. 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.

**IMPORTANTE!**

- Alcuni adattatori Wi-Fi potrebbero avere problemi a connettersi agli access point Wi-Fi 802.11be.
- Se incontrate questo problema assicuratevi di usare gli ultimi driver disponibili. Consultate il sito di supporto ufficiale del produttore per ottenere driver, aggiornamenti e ulteriori informazioni.
    - Realtek: https://www.realtek.com/en/downloads
    - Mediatek: https://www.mediatek.com/products/connectivity-and-networking/broadband-wifi
    - Intel: https://downloadcenter.intel.com/

# 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).

**AVVERTIMENTO!**

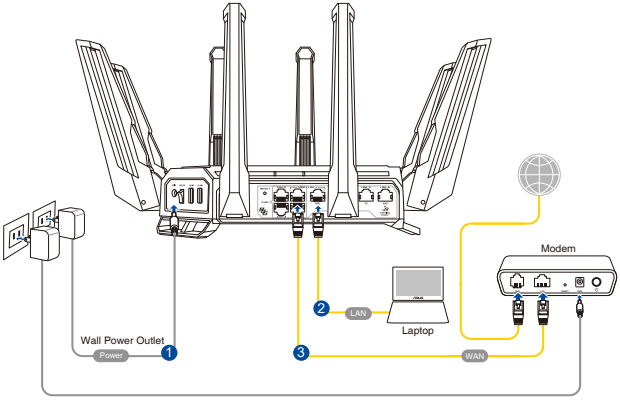
- Il cavo o i cavi di alimentazione devono essere inseriti a prese che sono dotate di un'adeguata messa a terra. Collegare l'apparecchio solo ad una presa vicina e facilmente accessibile.
- Se l'adattatore è danneggiato non provare a ripararlo. Contattate un tecnico qualificato o il vostro rivenditore.
- NON utilizzare cavi di alimentazione, accessori o periferiche danneggiate.
- NON montate questo dispositivo ad un'altezza superiore a 2 metri.
- Usa questo prodotto in ambienti la cui temperatura sia compresa tra 0°C(32°F) e 40°C(104°F).

## A. Connessione cablata

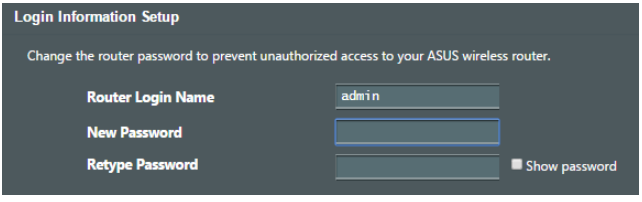
**NOTA:** Potete usare un cavo dritto, o incrociato (crossover), per la connessione cablata del PC al router.

### 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.



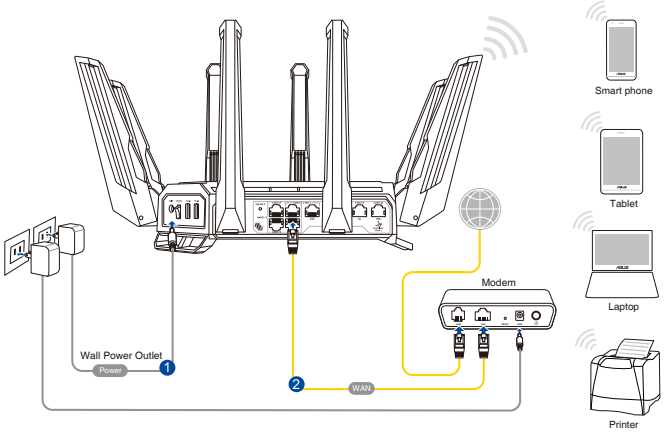

2. L'interfaccia web (GUI) si avvia automaticamente quando aprite un browser web. In caso contrario inserite http://www.asusrouter.com nella barra degli indirizzi.
3. Impostate una password per il vostro router per prevenire accessi non autorizzati.



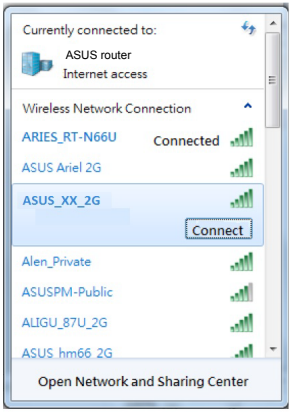
## B. Connessione senza fili

### 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.



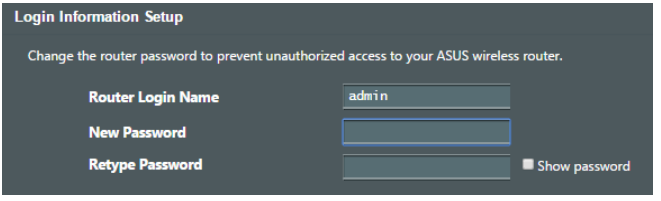

| | |
|---|---|
| Nome Wi-Fi 2.4G (SSID): | ASUS_XX_2G |
| Nome Wi-Fi 5G-1 (SSID): | ASUS_XX_5G-1 |
| Nome Wi-Fi 5G-2 (SSID): | ASUS_XX_5G-2 |
| Nome Wi-Fi 6G (SSID): | ASUS_XX_6G |

* **XX** corrisponde alle ultime due cifre dell'indirizzo MAC 2.4GHz. Potete trovare l'indirizzo sull'etichetta nel retro del router ROG.

3. Una volta eseguita la connessione l'interfaccia web (GUI) si avvia automaticamente quando aprite un browser web. In caso contrario inserite http://www.asusrouter.com nella barra degli indirizzi..
4. 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.



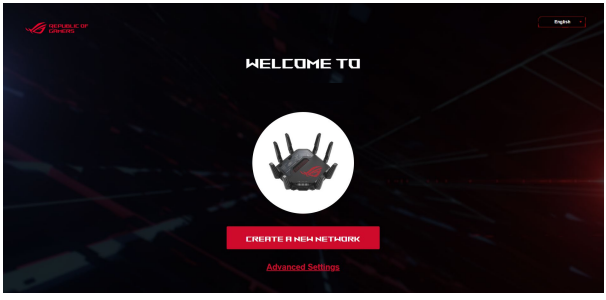
## 2.2 Installazione rapida Internet (QIS) con auto-rilevamento

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://www.asusrouter.com manualmente.



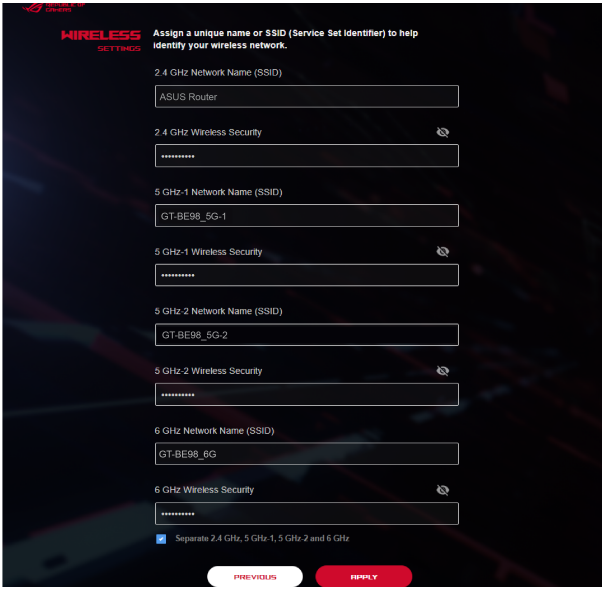

2. Il router è in grado di capire automaticamente se la connessione fornita dal vostro ISP è a **IP dinamico**, **PPPoE**, **PPTP** o **L2TP**. Inserite le informazioni necessarie per individuare il tipo di connessione fornita dal vostro ISP.

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

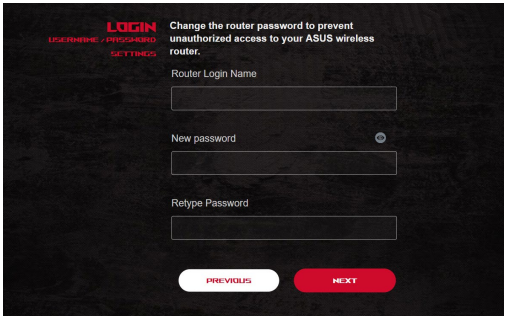
**NOTE:**

- 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, 5GHz-1, 5GHz-2 e 6GHz. Quando avete finito cliccate su **Apply (Applica)**.



4. 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-1/5GHz-2/6GHz. 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-1/5GHz-2/6GHz e le chiavi di sicurezza permettono ai dispositivi Wi-Fi di accedere e connettersi alle reti wireless 2.4GHz/5GHz-1/5GHz-2/6GHz.

## 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 per confermare la connessione.

**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 e avanzate

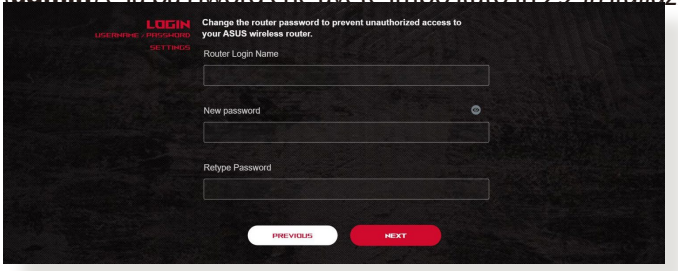
## 3.1 Accedere all'interfaccia web

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.

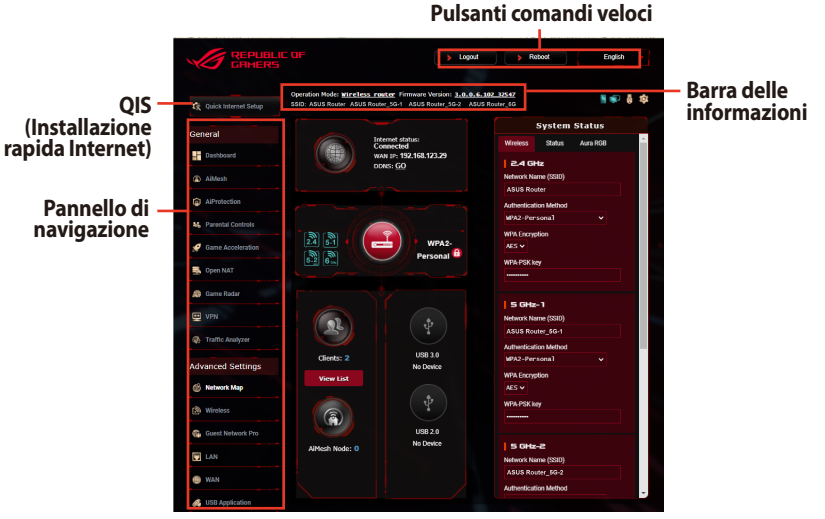
**NOTA:** Le caratteristiche possono variare in base alla versione del firmware installata sul router.

**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://www.asusrouter.com.
2. Nella pagina di accesso inserite il nome utente predefinito (**admin**) e la password che avete impostato in *2.2 Installazione*




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



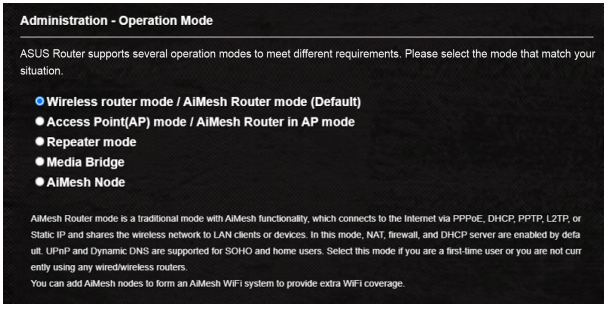

* L'immagine è solo di riferimento.

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

# 3.2 Amministrazione

## 3.2.1 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:
   - **Modalità Wireless router (Router wireless)/Modalità AiMesh Router (Router AiMesh) (impostazione 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 (AP) / AiMesh Router (Router AiMesh) in modalità AP:** In questo modo il router, collegato ad una rete cablata, crea una nuova rete wireless.
   - **Repeater Mode (Modalità ripetitore):** Nella modalità ripetitore GT-BE98 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.
   - **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.

- **Nodo 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.

### 3.2.2 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)**.

### 3.2.3 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 **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 *4.2 Firmware Restoration* per avere maggiori informazioni su come effettuare il recupero del firmware.

### 3.2.4 Ripristina/Salva/Carica Impostazioni

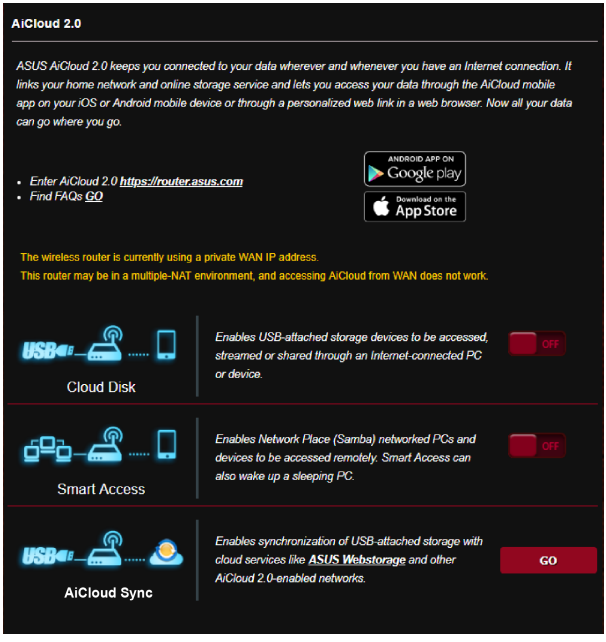
**Per ripristinare/salvare/caricare le impostazioni del router wireless:**

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate)** > **Administration (Amministrazione)** e selezionate la **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 (Sfoglia)**, selezionate il vostro file e poi cliccate su **Upload (Carica)** se volete ripristinare le impostazioni che avete precedentemente salvato su un file.

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

## 3.3 AiCloud 2.0

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



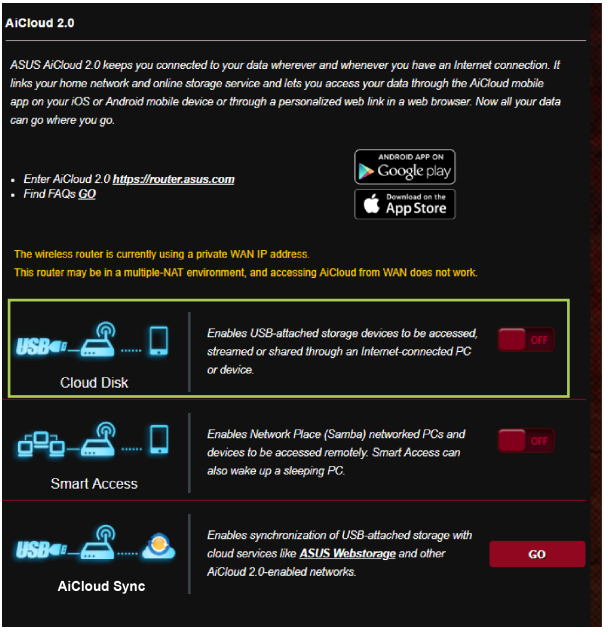

### Per usare AiCloud:

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.

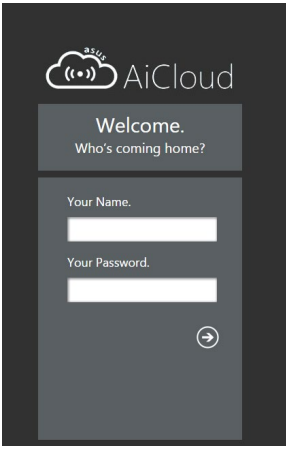
## 3.3.1 Disco Cloud

### 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**.

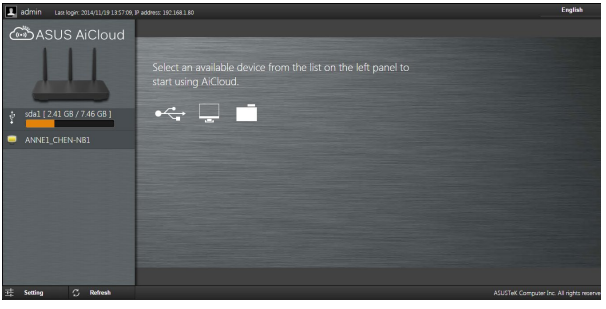


3. Andate su http://www.asusrouter.com e inserite il nome utente e la password per l'accesso al router. Raccomandiamo di utilizzare **Google Chrome** o **Mozilla Firefox** per un'esperienza migliore.



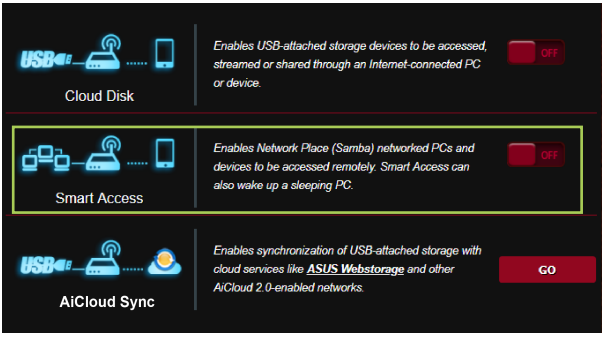

4. Potete ora avere accesso ai file presenti sui dischi cloud dei dispositivi connessi alla vostra rete.

**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.



### 3.3.2 Smart Access

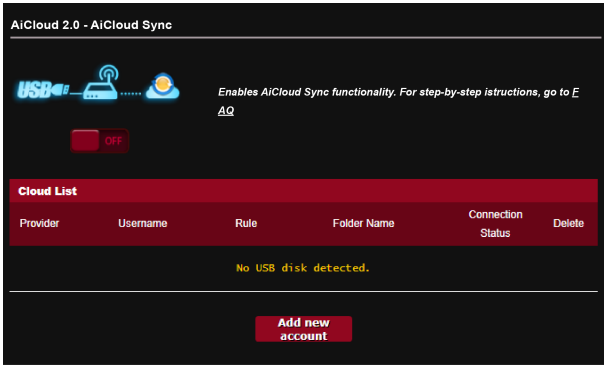
La funzione Smart Access permette di accedere facilmente alla vostra rete domestica tramite il nome di dominio del vostro router.




**NOTE:**

- Potete creare un nome di dominio per il vostro router usando ASUS DDNS. Per maggiori dettagli fate riferimento alla sezione *3.21.6 DNS Dinamico*.
- Come impostazione standard AiCloud stabilisce una connessione sicura HTTPS. Inserite il vostro account https://[accountASUSDDNS].asuscomm.com per un utilizzo sicuro di Cloud Disk e Smart Access.

### 3.3.3 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)**.

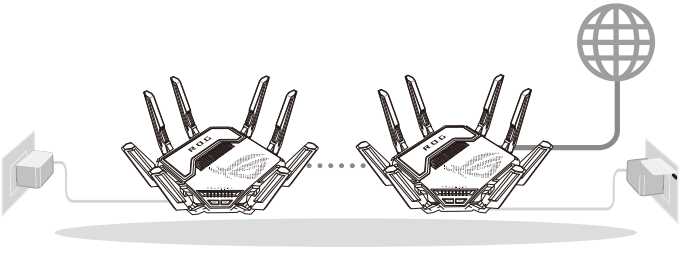
# 3.4 ASUS AiMesh

## 3.4.1 OPERAZIONI PRELIMINARI

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.



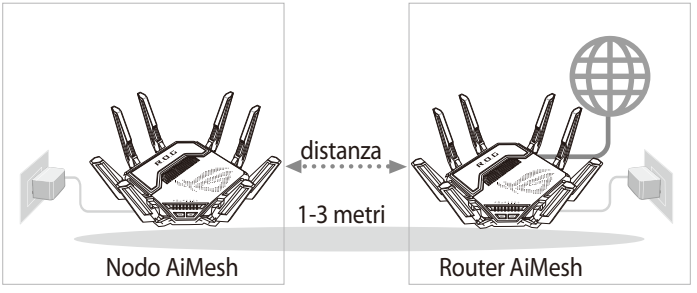

## 3.4.2 Configurazione di AiMesh.

**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.

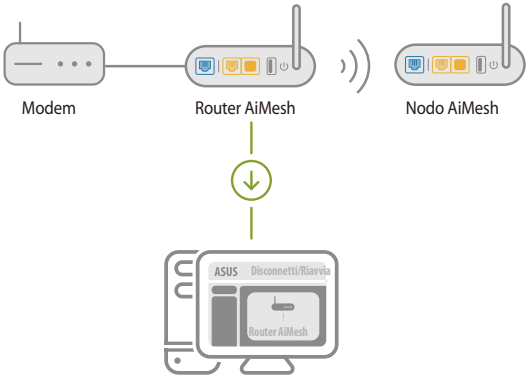
**Nodo AiMesh**

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



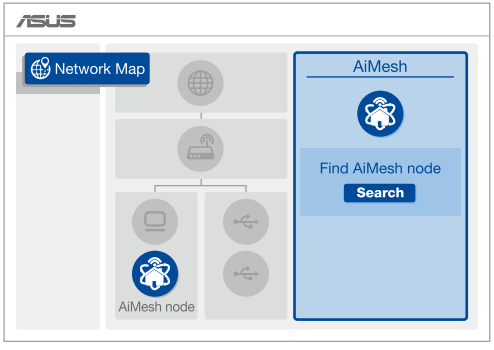
## Router AiMesh

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



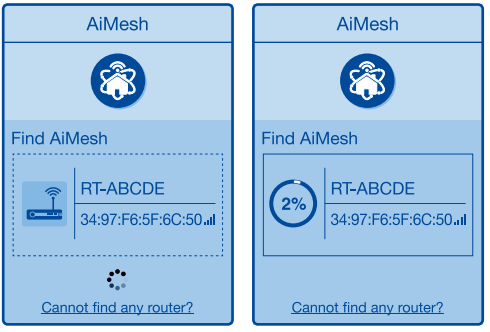

2) Andate alla pagina **Mappa di rete**, cliccate sull'icona AiMesh e poi su **Cerca** per cercare il nodo AiMesh.

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

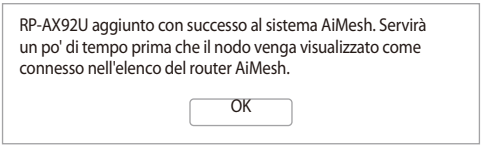


3) Cliccate su **Cerca**, il sistema cercherà automaticamente il vostro nodo AiMesh. Quando il nodo AiMesh verrà rilevato e visualizzato su questa pagina cliccate su di esso per aggiungerlo al sistema AiMesh.

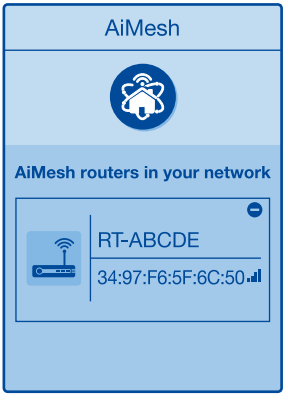
**NOTA:** Se non riuscite a trovare alcun nodo AiMesh andate alla sezione **RISOLUZIONE DEI PROBLEMI**.




4) A sincronizzazione completata verrà visualizzato un messaggio.



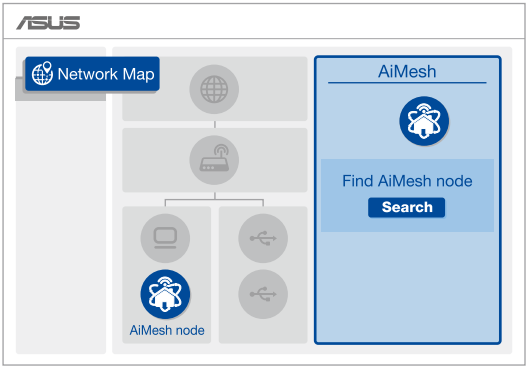

5) Congratulazioni! Quando un nodo AiMesh viene aggiunto correttamente alla rete AiMesh verrà visualizzato un messaggio di questo tipo.



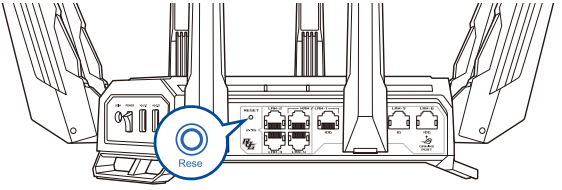
### 3.4.3 Troubleshooting

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

1) Spostate nodo AiMesh più vicino al router AiMesh. Assicuratevi che i dispositivi siano ad una distanza compresa tra 1 e 3 metri.
2) Nodo AiMesh è acceso.
3) Il vostro nodo AiMesh è dotato di un firmware che supporta 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://www.asusrouter.com
   iv. ndate su **Amministrazione > Aggiornamento del firmware**. Cliccate su **Seleziona 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.




### 3.4.4 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.


### 3.4.5 Domande e risposte frequenti (FAQ)

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

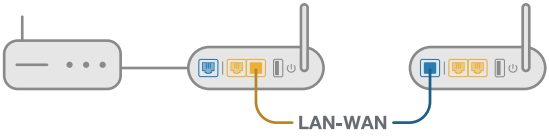
**A:** Sì. Potete scegliere di configurate il router AiMesh nelle modalità router o access point. Entrate nell'interfaccia web (GUI) (http://www.asusrouter.com) e andate su **Amministrazione** > **Modalità operativa**.

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

**A:** Sì. Il sistema AiMesh supporta entrambe le connessioni cablata 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..



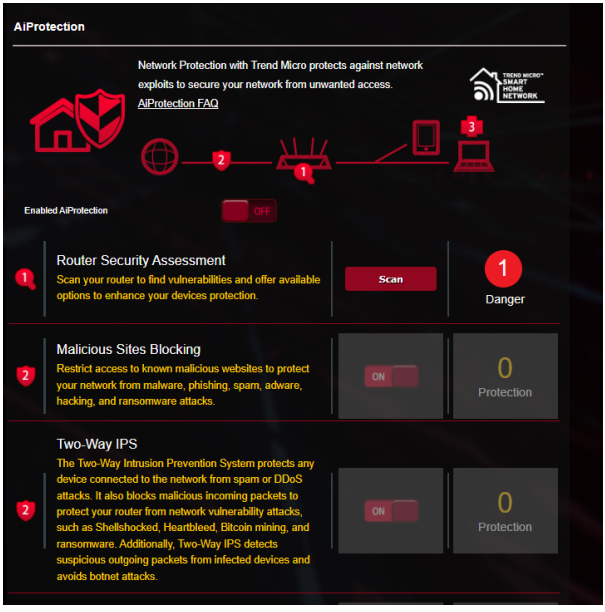

3) Il sistema AiMesh selezionerà automaticamente il percorso migliore per la trasmissione dei dati.

## 3.5 AiProtection

AiProtection 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.

## 3.5.1 Configurazione di AiProtection

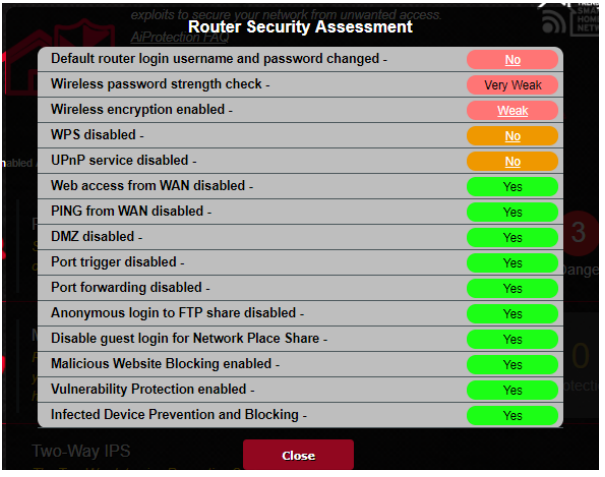
AiProtection permette di proteggersi contro exploit di rete per impedire accessi non autorizzati.



**Per configurare AiProtection:**

1. Dal pannello di navigazione andate su **General (Generale)** > **AiProtection**.
2. Nella pagina principale di **AiProtection** cliccate su **Network Protection (Protezione della rete)**.
3. Nella scheda di **Network Protection** 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. Cliccate su **OK** al messaggio di conferma.

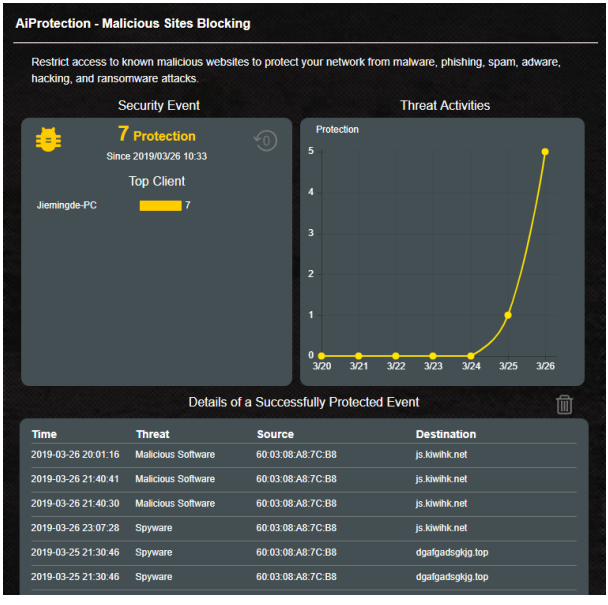
## 3.5.2 Blocco siti web malevoli

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**.
2. Nella pagina principale di **AiProtection** cliccate su **Network Protection (Protezione della rete)**.
3. Nel pannello di **Malicious Sites Blocking (Blocco siti web malevoli)** cliccate su **ON**.



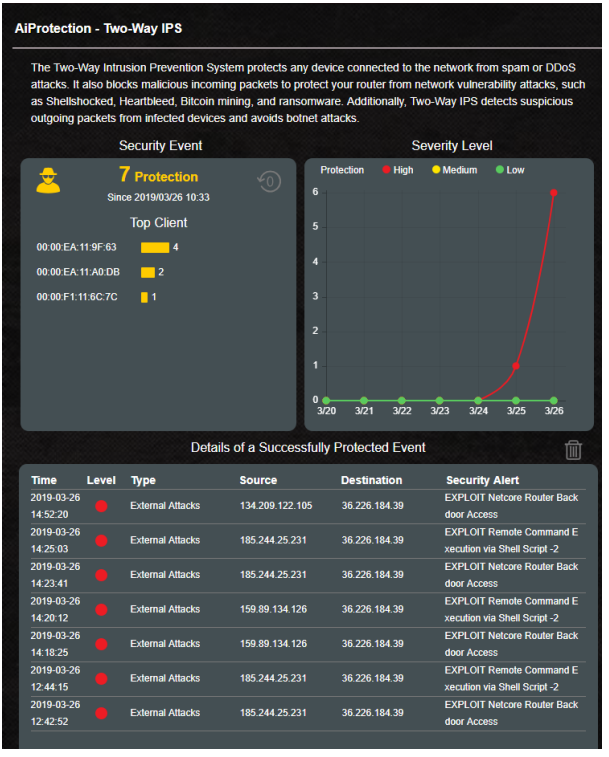
## 3.5.3 IPS bidirezionale

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**.
2. Nella pagina principale di **AiProtection** cliccate su **Network Protection (Protezione della rete)**.
3. Nel pannello di **Two-Way IPS (IPS bidirezionale)** cliccate su **ON**.



### 3.5.4 Prevenzione e blocco di dispositivi infetti

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

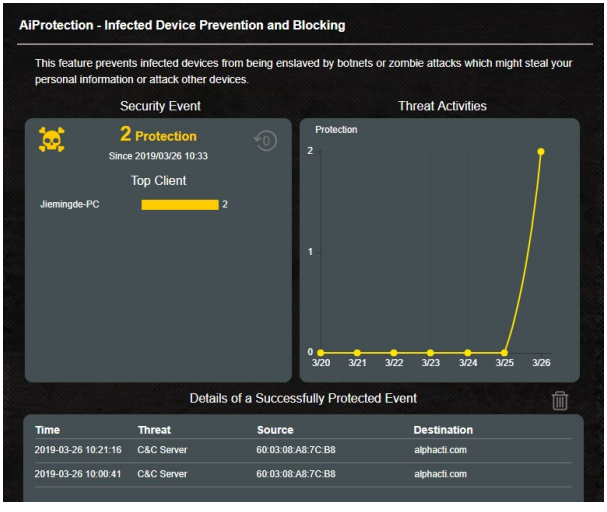
**NOTA:** Questa funzione viene abilitata automaticamente se eseguite la **Router Weakness Scan (Scansione vulnerabilità del router)**.

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

1. Dal pannello di navigazione andate su **General (Generale)** > **AiProtection**.
2. Nella pagina principale di **AiProtection** 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**.

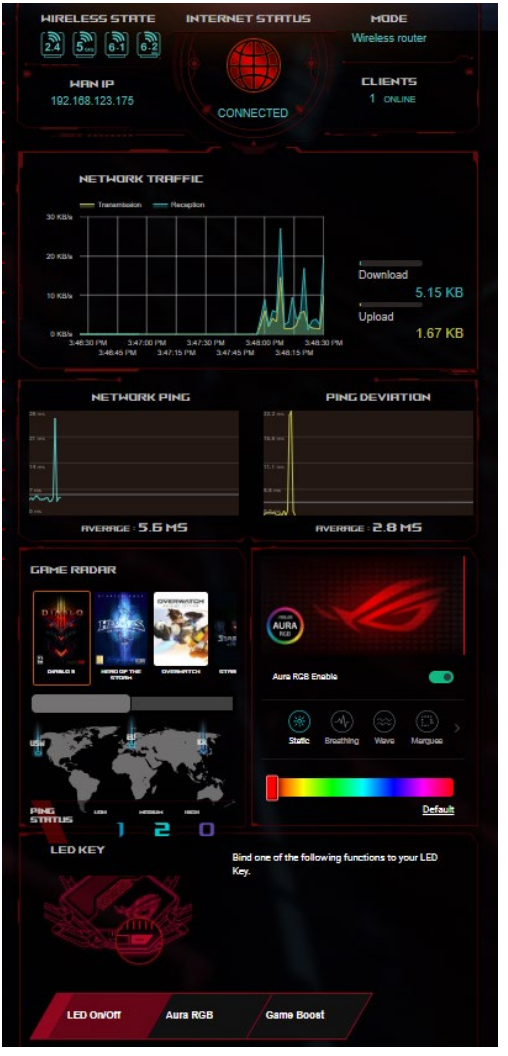
**Per configurare Preferenze avvisi:**

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)**.



## 3.6 Dash Board

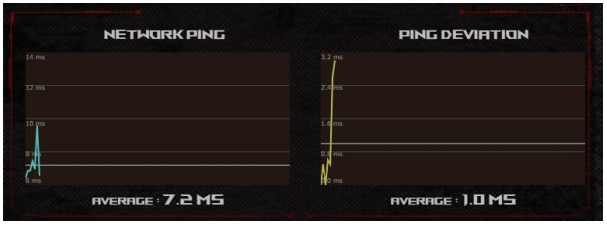
La Dashboard vi permette di monitorare il traffico in tempo reale per il vostro ambiente di rete e analizzare il ping in tempo reale e la deviazione del ping.



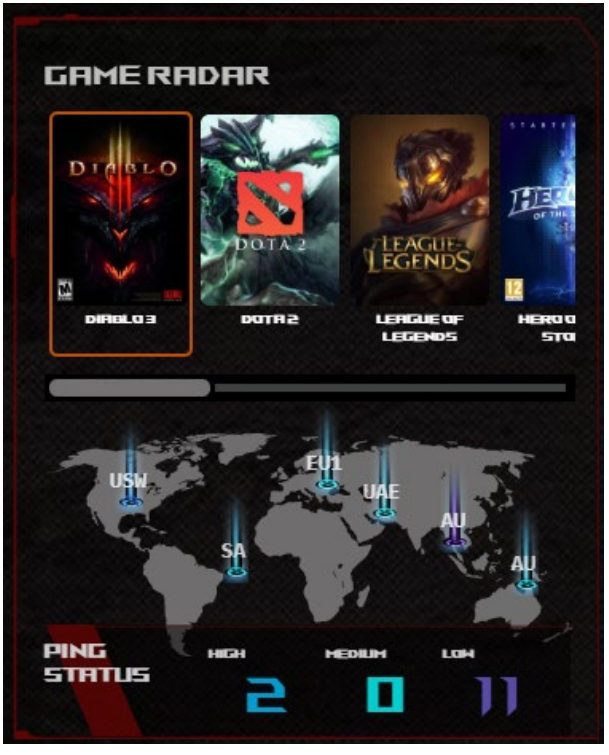

Il ping di rete è importante per le esperienze di gioco online. Un ping elevato si traduce in una latenza elevata per i giochi real-time. Per la maggior parte dei giochi online un ping di rete inferiore a 99 ms è considerato di buona qualità. Se il ping è inferiore a 150 ms la qualità

è accettabile. In via generale se il ping è più elevato di 150 ms diventa difficile giocare con fluidità.

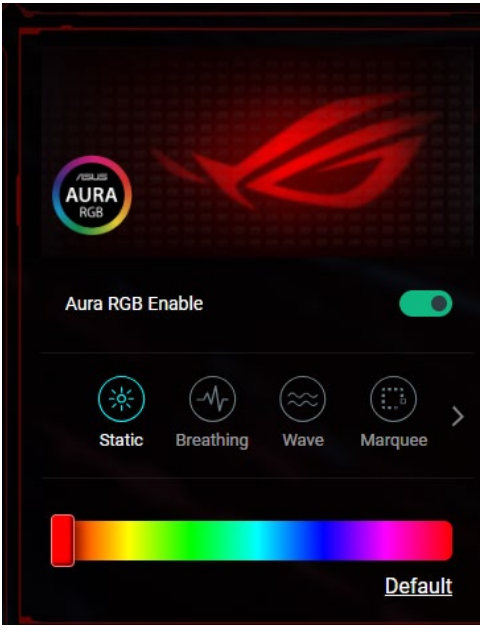
Anche la deviazione del ping è importante per le esperienze di gioco online. Con una deviazione del ping elevata è possibile andare incontro ad interruzioni durante il gioco online. Non c'è alcun criterio di base per la deviazione del ping. Tuttavia una deviazione del ping bassa è sempre preferibile.



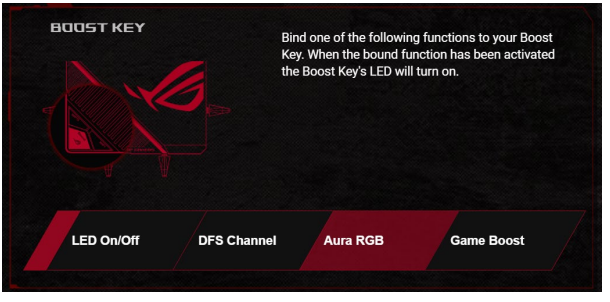

- **Game Radar:** La funzione Game Radar può dare informazioni rapide sulla latenza di un server specifico.



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




- **Tasto LED:** Il router gaming ROG Rapture è dotato del tasto LED, configurabile in base alle esigenze dell'utente.
  - LED acceso/spento
  - Aura RGB acceso/spento
  - Game Boost: abilita/disabilita priorità elevata per il traffico di gioco.



## 3.7 Firewall

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

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

### 3.7.1 Generale

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

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate)** > **Firewall** > **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)**.

### 3.7.2 Filtro URL

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

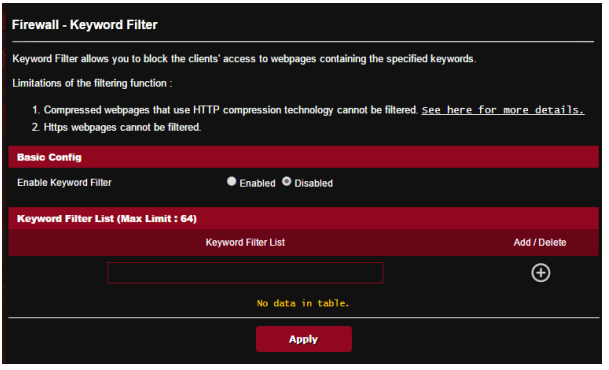
**NOTA:** Il filtro URL lavora sulle query DNS. Se un client ha già effettuato l'accesso ad un sito web, ad esempio http://www.abcxxx.com, potrà comunque visitare nuovamente il sito anche se il filtro lo impedirebbe (la cache DNS del sistema ricorda i siti visitati in precedenza in modo da non dover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

## 3.7.3 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:**

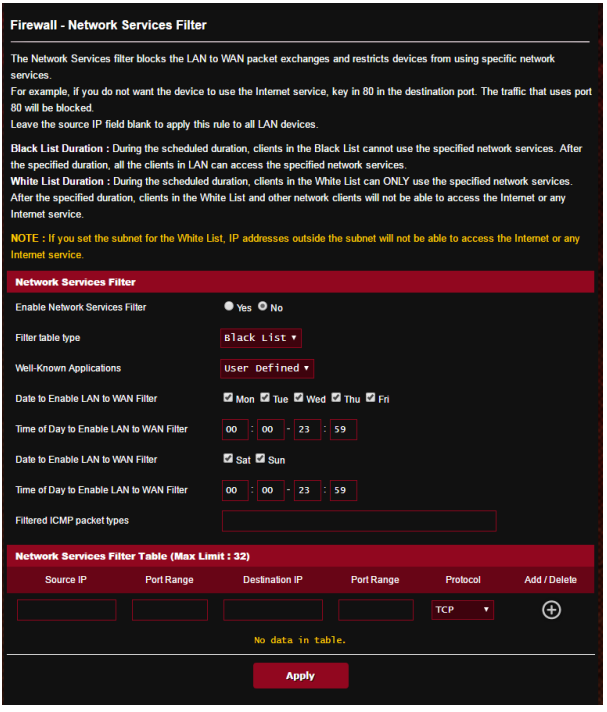
1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate)** > **Firewall** > **Keyword Filter (Filtro parole chiave)**.
2. Alla voce **Enable Keyword Filter (Abilita Filtro Parole Chiave)** selezionate **Enable (Abilita)**.
3. Inserite una parola o una frase e poi cliccate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

## 3.7.4 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.

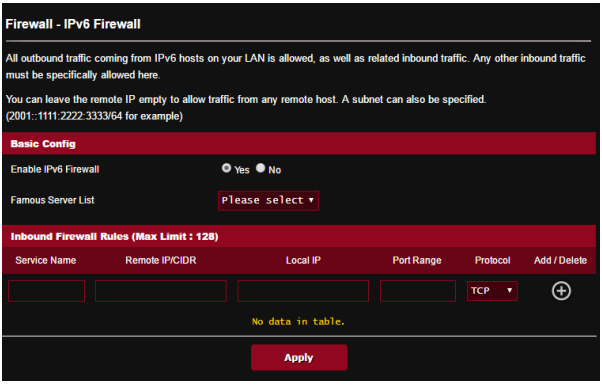



### Per abilitare e configurare il Packet Filter:

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate)** > **Administration (Amministrazione)** > **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)**.

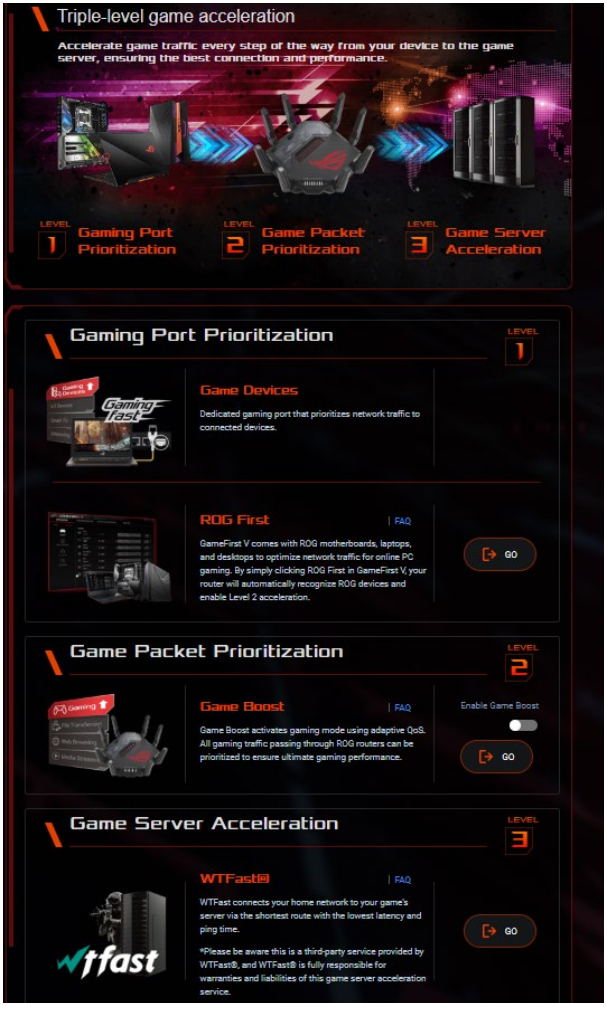
## 3.7.5 Firewall IPv6

Come impostazione standard il vostro router wireless ASUS blocca tutti il traffico in ingresso non richiesto. La funzione firewall IPv6 permette al traffico in ingresso proveniente da servizi specifici di entrare nella vostra rete.



## 3.8 Accelerazione del 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.



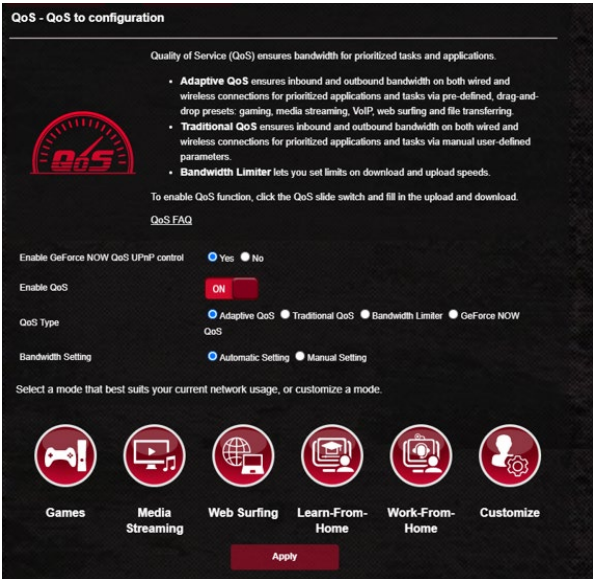

### Game Boost

**Per abilitare Game Boost:**

Nella **Game Boost** spostare il cursore **Enable Game Boost (Abilita Game Boost)** su **ON**.

### 3.8.1 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)** > **Accelerazione del gioco** > **QoS**.
2. Nel pannello di **Abilitare QoS** cliccate su **ON**.
3. 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.

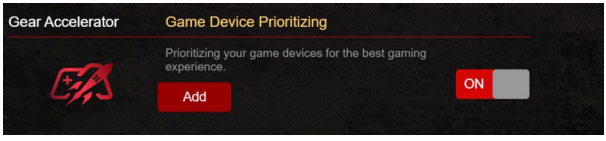
4. Fare clic su **Automatic Setting (Impostazione automatica)** per la larghezza di banda ottimale automaticamente o su **Manual Setting (Impostazione manuale)** per impostare manualmente la larghezza di banda di upload e download.

   **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.

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

### 3.8.2 Gear Accelerator

Gear Accelerator vi permette di assegnare priorità elevata ai dispositivi gaming tramite il pannello di controllo online, per un'esperienza gaming senza pari.



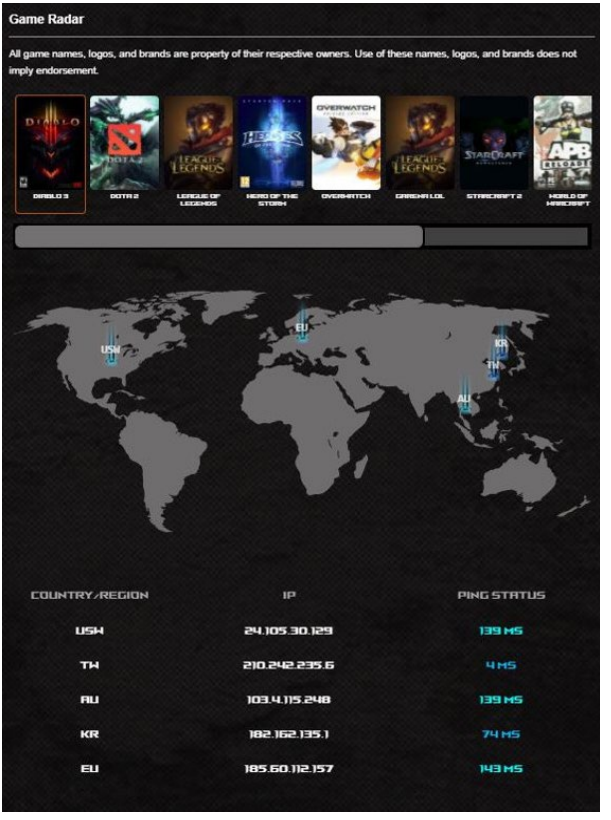

**Per configurare Gear Accelerator:**

1. Dal pannello di navigazione andate su **General (Generale)** > **Accelerazione del gioco**.
2. Nella scheda di **Gear Accelerator** spostate il cursore su **ON**.
3. Dopo aver applicato le impostazioni cliccate su **Add** per selezionare il nome del client.
4. Cliccate su per aggiungere il profilo del client.
5. Cliccate su **Apply (Applica)** per confermare le modifiche

**NOTA:** Se volete eliminare il profilo del client cliccate su .

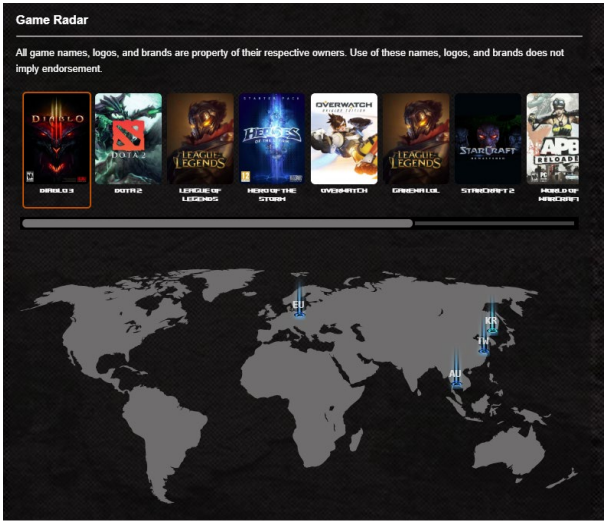
## 3.9 Game Radar

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




**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.

## 3.10 Rete guest Pro

Rete guest Pro è una versione avanzata della Rete guest configurata all'interno di una rete più ampia, solitamente a casa o in ufficio. Rete guest Pro viene generalmente utilizzato per fornire accesso a Internet a visitatori o ospiti senza consentire loro di accedere alla rete principale o ad altri dispositivi connessi. Fornisce inoltre un filtro dei contenuti di rete utilizzato per bloccare o consentire l'accesso a determinati tipi di contenuti online su una rete.

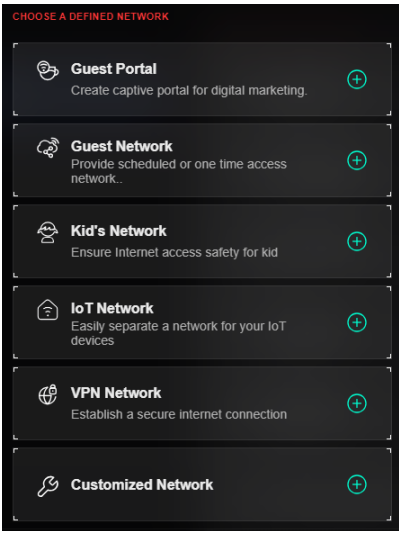
- **Portale guest:** Crea un Captive Portal per il marketing digitale.
- **Rete guest:** Crea una rete guest con una pianificazione WiFi e diritti di accesso per controllare quando e come gli ospiti possono utilizzare la rete.
- **Rete per bambini:** Crea una rete per bambini che blocca l'accesso ai contenuti per adulti* e dispone di una pianificazione per controllare quando la rete è disponibile.
- **Rete IoT:** Crea una rete Internet of Things (IoT) che blocca il traffico dannoso* e consente la connessione solo ai dispositivi a 2.4 GHz.
- **Rete VPN:** Crea una rete VPN che si connette a servizi VPN di terzi o utilizza la VPN da sito a sito ASUS (https://www.asus.com/support/FAQ/1048281/) per crittografare la connessione Internet e nascondere l'indirizzo IP dell'utente per proteggere le attività online ed evitare che vengano tracciate o monitorate.

**NOTE:**

- GT-BE98 supporta fino a 5 SSID multipli (2,4 GHz + 5 GHz).
- Quando viene creata una Rete guest Pro, si crea anche una VLAN nelle impostazioni VLAN.
- Il filtro dei contenuti è alimentato da servizi basati su DNS.

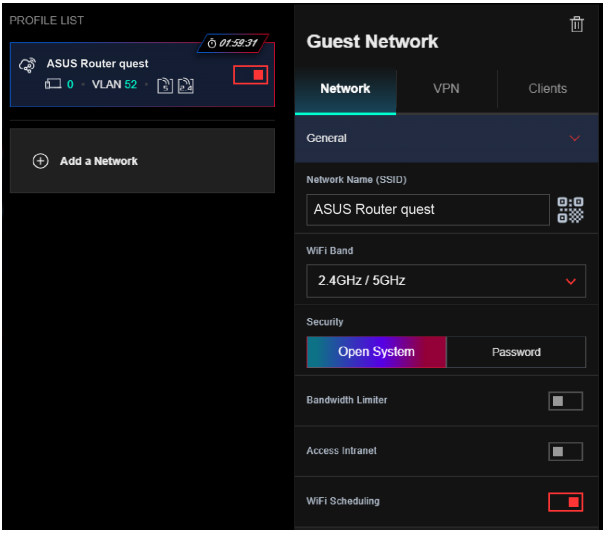
**Per configurare una Rete guest Pro:**

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate)** > **Guest Network Pro (Rete guest Pro)**.
2. Fare clic su **Add a Network (Aggiungi rete)** per creare una Rete guest Pro.

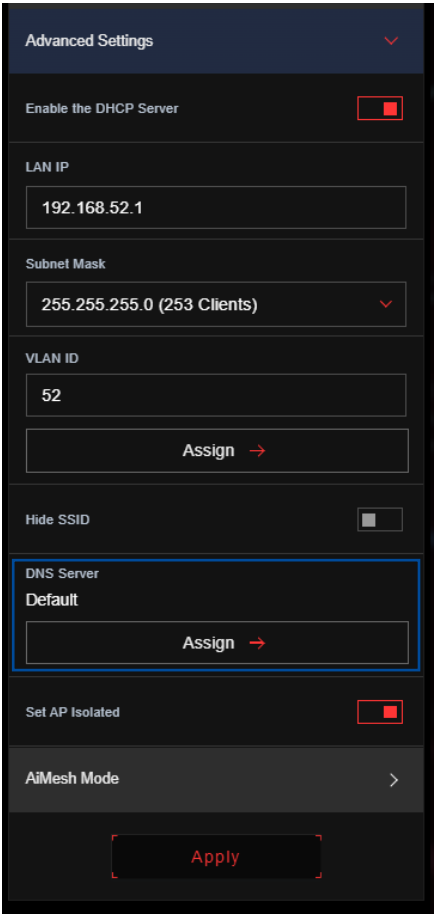



**Per assegnare un filtro in Rete guest Pro:**

1. Creare una Rete guest Pro o selezionarne una dall'elenco.
2. Fare clic su **Advanced Settings (Impostazioni avanzate)**.

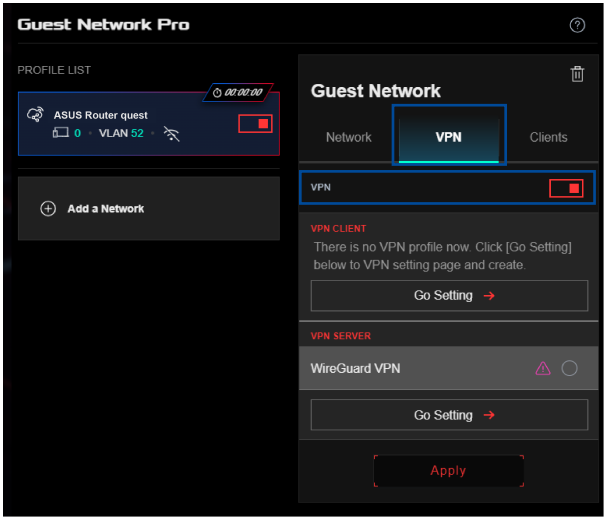


3. **Assegnare** un server DNS da utilizzare o immettere un server DNS personalizzato.
4. Cliccate su **Apply (Applica)** per confermare le modifiche.

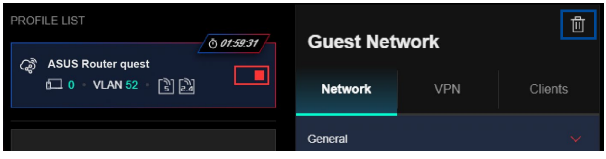


**Per assegnare una VPN in Rete guest Pro:**

1. Creare una Rete guest Pro o selezionarne una dall'elenco.
2. Fare clic sulla scheda **VPN** e abilitarla.
3. Selezionare una VPN dall'elenco. Se sul router non è presente alcun client VPN, fare clic su **Go Setting (Vai a Impostazione)** e attenersi alle istruzioni visualizzate per crearne uno.
4. Cliccate su **Apply (Applica)** per confermare le modifiche.

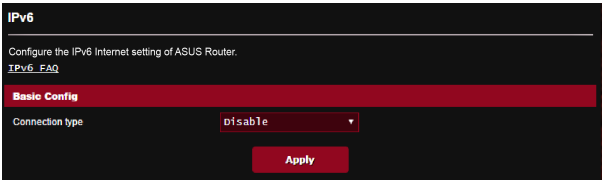



**NOTA:** È possibile fare clic sulle impostazioni di un profilo per modificarlo o fare clic su nell'angolo in alto a destra per eliminarlo.



## 3.11 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)**.

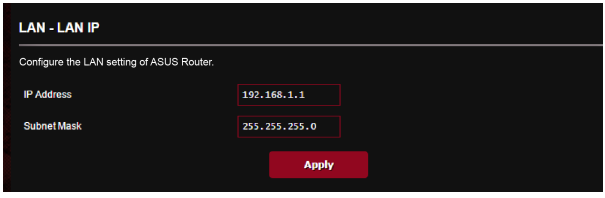
**NOTA:** Chiedete informazioni al vostro ISP per sapere se IPv6 è effettivamente supportato.

# 3.12 LAN

## 3.12.1 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.

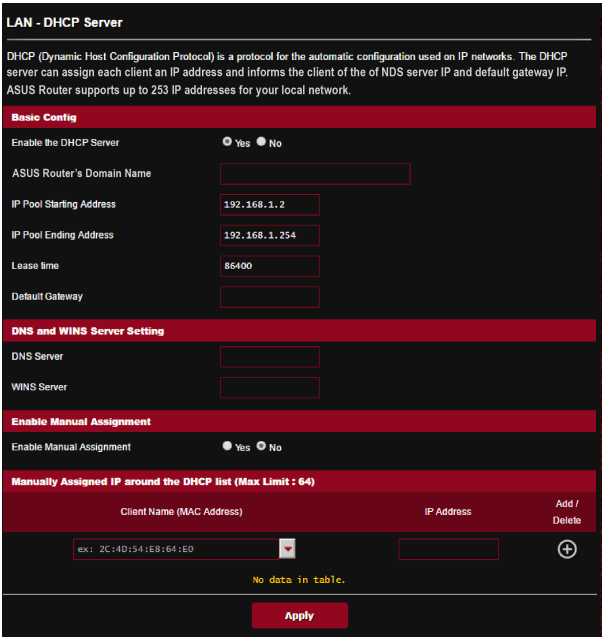



**Per modificare le impostazioni LAN del router wireless:**

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

## 3.12.2 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 **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:**

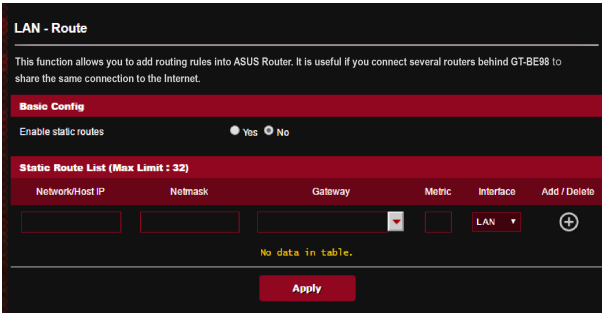
- Raccomandiamo di utilizzare un indirizzo IP del formato 192.168.1.xxx (con xxx che può variare da 2 a 254) quando dovete scegliere un intervallo di indirizzi IP.
- L'indirizzo IP iniziale non deve essere superiore all'indirizzo IP finale.

7. Nella sezione **DNS and Server Setting (Impostazione DNS e Server)** 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.

## 3.12.3 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.

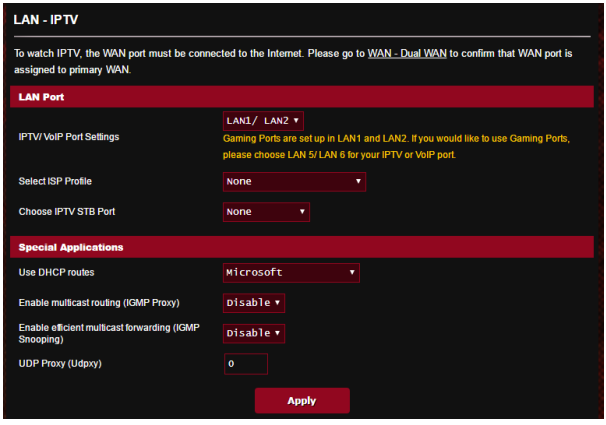



**Per configurare la tabella di routing:**

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate)** > **LAN** > **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)**.

## 3.12.4 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.

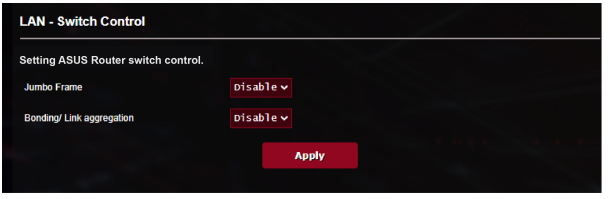


## 3.12.5 Controllo dello switch

Consente di configurare il router per la funzione di controllo dello switch. È possibile combinare due porte 10 Gbps per offrire velocità cablate fino a 20 Gbps tramite connessione al NAS compatibile o ad un altro dispositivo di rete a larghezza di banda elevata.

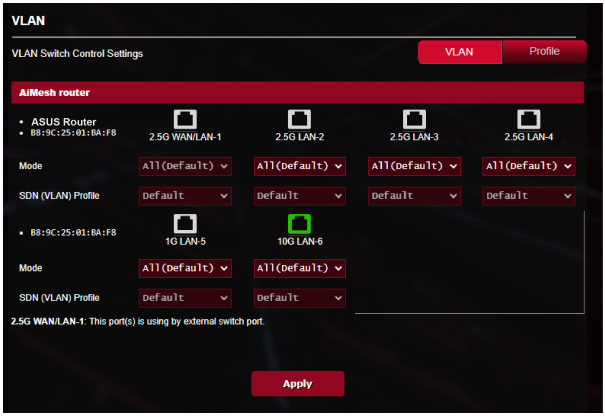
**NOTE:**

- Per utilizzare la funzione LACP (Link Aggregation Control Protocol), i dispositivi devono supportare il protocollo IEEE 802.3ad.
- La funzione di aggregazione LAN può essere utilizzata associando le due porte da 10 Gbps.



## 3.12.6 VLAN

Una VLAN (Virtual Local Area Network) è una rete logica creata all'interno di una rete fisica di maggiori dimensioni. Le VLAN consentono di segmentare una rete in sottoreti virtuali di dimensioni inferiori, che possono essere utilizzate per isolare il traffico e migliorare le prestazioni della rete.




**Per configurare VLAN:**

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate)** > **LAN** > **VLAN**.
2. Fare clic sulla scheda Profilo, quindi su ⊕ per creare un profilo VLAN. È possibile assegnare il proprio ID VLAN.
3. **Port isolation (Isolamento porta)** limita il diritto di accesso di diversi dispositivi nella stessa VLAN. Ora si sta creando una "Rete solo VLAN", ovvero una rete con VID, ma senza DHCP.
4. Fare clic sulla scheda **VLAN** per selezionare una porta con profilo e modalità specifici (**Trunk** / **Access**) (**(Trunk/Accesso)**).

**NOTA:** È possibile selezionare una delle seguenti modalità predefinite:

**Tutto (predefinito)** consente l'accesso a tutti i pacchetti con tag e senza tag.

La modalità di **accesso** consente l'accesso a una SDN(VLAN) selezionata. È possibile selezionare i profili creati da Guest Network pro o da VLAN.

Modalità **Trunk**:

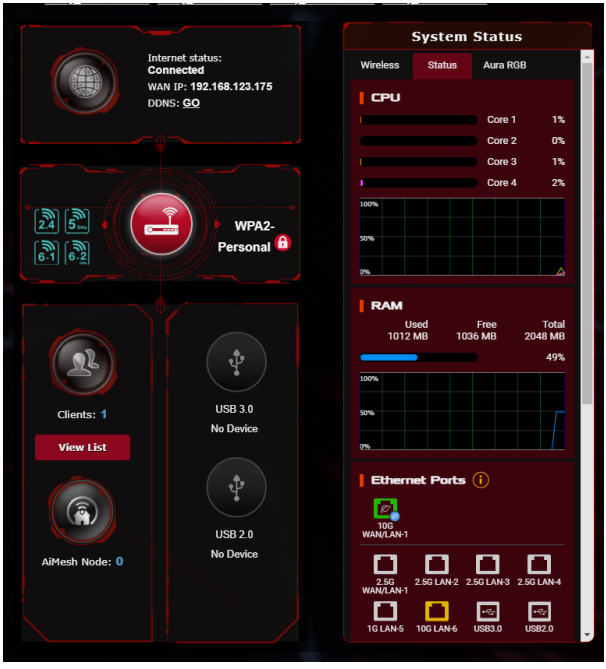
- **Consenti tutti i pacchetti con tag:** È consentito l'accesso a tutti i pacchetti con tag.
- **Con SDN(VLAN) selezionata:** È consentito l'accesso a una sola SDN o VLAN selezionata.

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

**NOTA:** Per altre informazioni, visitare https://www.asus.com/support/FAQ/1049415/.

## 3.13 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.




### 3.13.1 Configurare le impostazioni di protezione della rete wireless

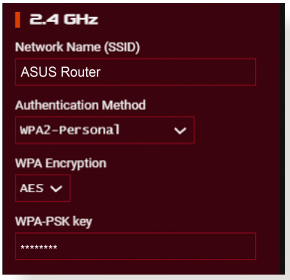
Per proteggere la vostra rete wireless dagli accessi non autorizzati dovete configurare le sue impostazioni di protezione.

**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 tre diverse bande di frequenza 2.4GHz, 5GHz-1, 5GHz-2 e 6GHz.

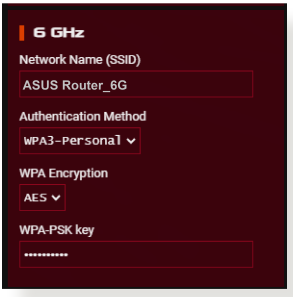
### Impostazioni di protezione 2.4GHz




### Impostazioni di protezione 5GHz-1


### Impostazioni di protezione 5GHz-2


### Impostazioni di protezione 6GHz



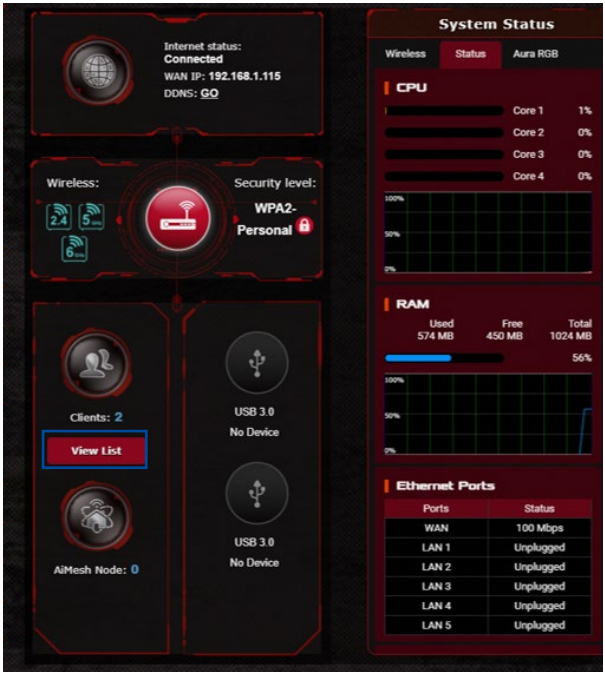

3. Nel campo **Network Name (Nome della rete) (SSID)** inserite un nome unico da assegnare alla vostra rete wireless.
4. Dall'elenco **Authentication Method (Metodo d'autenticazione)** selezionate la modalità di autenticazione per la vostra rete wireless.

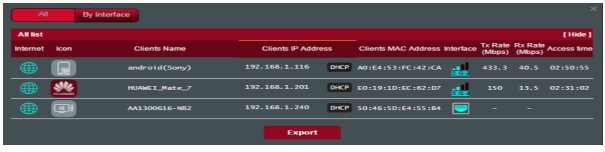
   Se selezionate WPA/WPA2/WPA3-Personal inserite la chiave WPA-PSK o la passkey di sicurezza.

**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)**.

## 3.13.2 Gestione dei client di rete



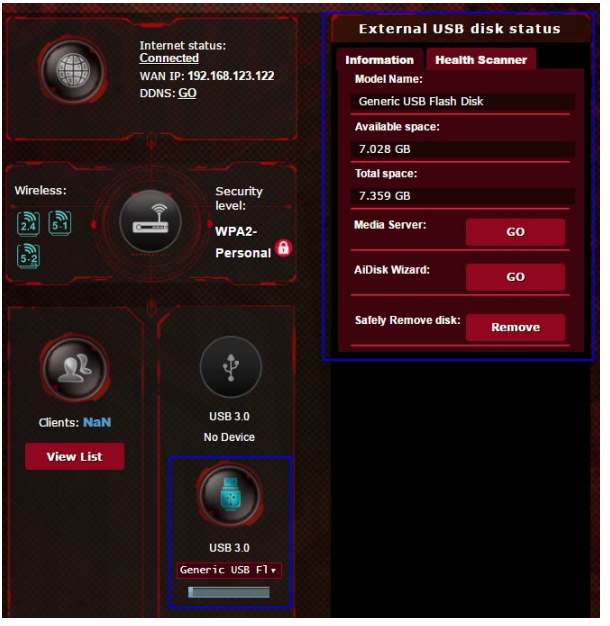




**Per gestire i client della vostra rete:**

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.

### 3.13.3 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, Samba o AiCloud. Per maggiori dettagli fate riferimento alle sezioni *3.19 Applicazioni USB* e *3.3 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:**

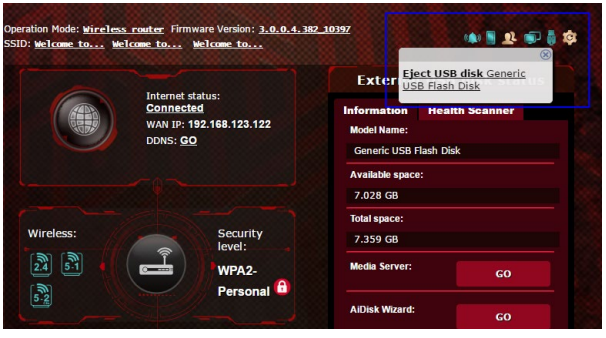
- Per maggiori dettagli fate riferimento alla sezione *3.19.2 Utilizzare il centro Gestione Server* di questo manuale.
- Il router wireless supporta la maggior parte dei dischi USB e delle memorie flash USB (fino a 4 TB di dimensione) e supporta accesso in lettura e in scrittura sui file system FAT16, FAT32, NTFS e HFS+.

## Per effettuare una 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:**

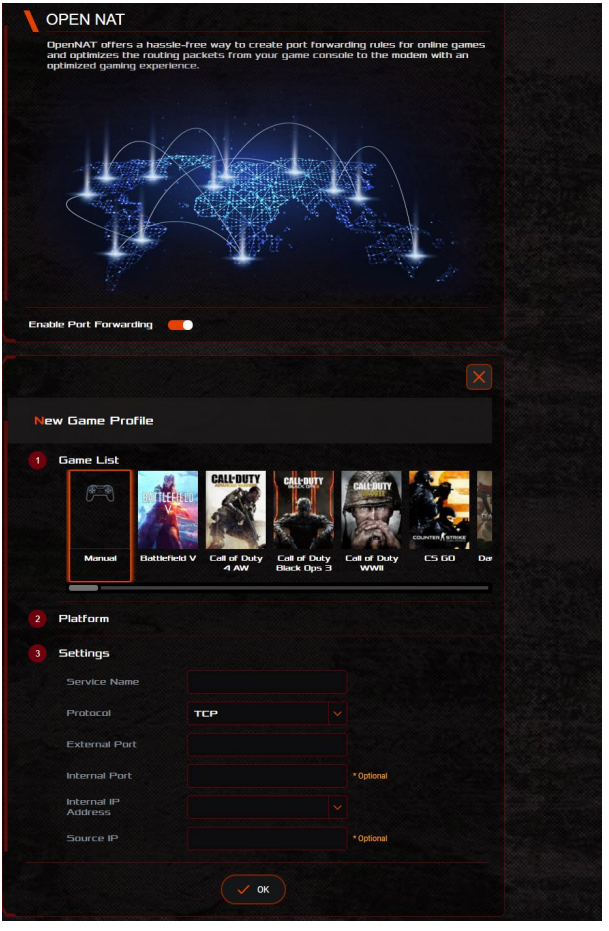
1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate)** > **Network Map (Mappa di rete)**.
2. Nell'angolo in alto a destra cliccate su  > **Eject USB disk (Espelli disco USB)**. Quando il disco USB è stato rimosso correttamente il campo USB Status (Stato USB) mostrerà il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



## 3.14 Open NAT e Game Profile (Profilo gioco)

Open NAT offre un modo semplice per creare regole di port forwarding per i giochi online e ottimizza i pacchetti di routing dalla console di gioco al modem con un'esperienza di gioco ottimizzata.

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:**

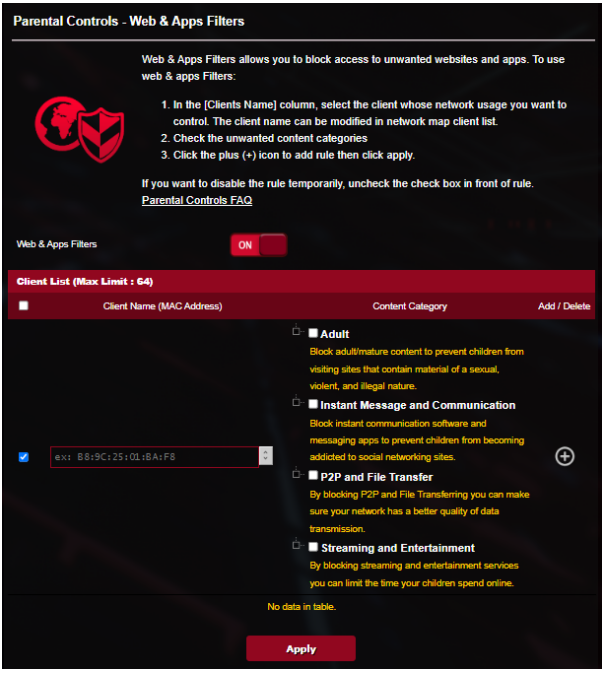
1. Dal pannello di navigazione andate su **General (Generale)** > **Open NAT**.
2. Scorrere su **Enable Port Forwarding (Abilita Port forwarding)**.
3. Da **Game List (Elenco giochi)**, selezionare un gioco e completare le impostazioni di base.
4. Cliccate su **OK**.

## 3.15 Controllo Genitori

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

**Per abilitare IPS bidirezionale:**

Dal pannello di navigazione andate su **General (Generale)** > **Parental Controls (Controllo genitori).**




### 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:**

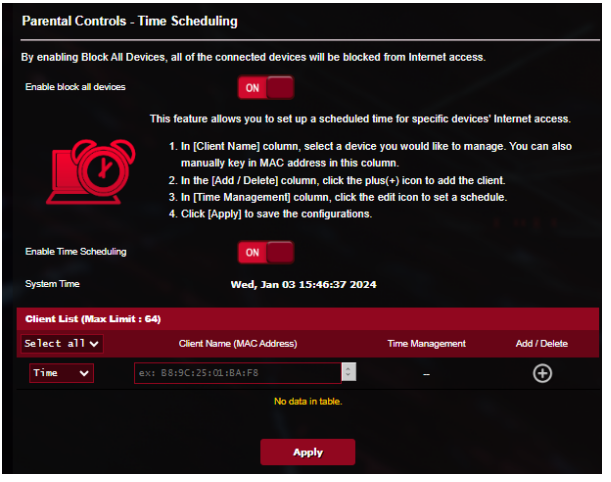
1. Dal pannello di navigazione andate su **General (Generale)** > **Parental Controls (Controllo genitori).**
2. Nel pannello di **Web & Apps Filters (Filtro web e app)** cliccate su **ON**.

3. Quando appare il messaggio con il contratto di licenza per l'utente finale (EULA) cliccate su I agree (Accetto) per continuare.
4. Nella colonna **Client List (Elenco client)** selezionate o inserite il nome del client.
5. 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**.
6. Cliccate su ⊕ per aggiungere il profilo del client.
7. 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)** > **Parental Controls (Controllo Genitori)** > **Time Scheduling (Pianificazione temporale)**.
2. Nel pannello di **Enable Time Scheduling (Abilita Pianificazione temporale)** cliccate su **ON**.
3. Nella colonna **Client 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.

## 3.16 Smart Connect

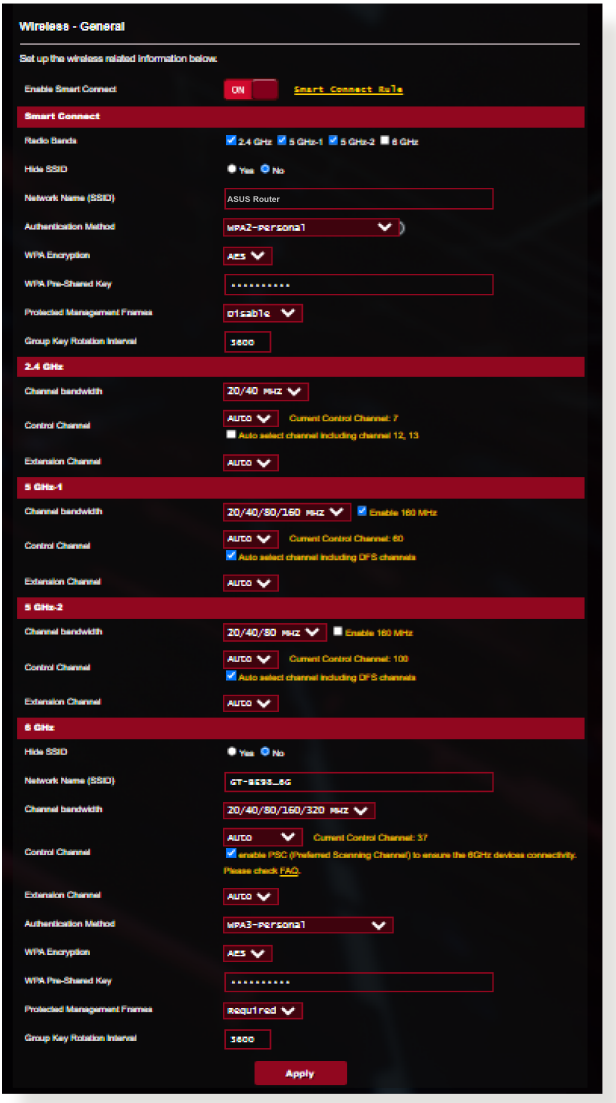
Smart Connect è progettato per pilotare automaticamente i client a una delle quattro frequenze disponibili (2.4 GHz, 5 GHz-1, 5 GHz-2, 6GHz).

### 3.16.1 Configurazione di Smart Connect

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

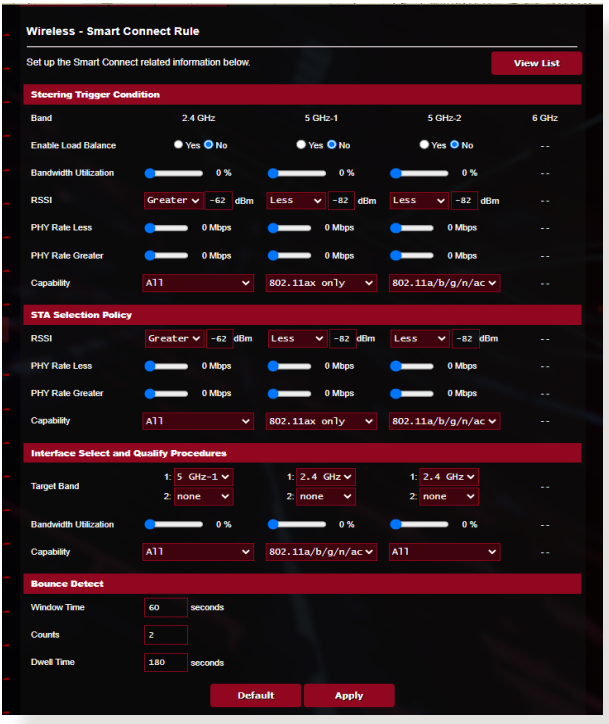
- ***Tramite la schermata Wireless***

1. Avviate il vostro browser e inserite, nella barra degli indirizzi, l'indirizzo standard del router: http://www.asusrouter.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** > **General (Generale)**.
4. Spostate 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.


Wireless - General
Set up the wireless related information below.
Enable Smart Connect
ON
Smart Connect Rule
Smart Connect
Radio Bands
2.4 GHz
5 GHz-1
5 GHz-2
6 GHz
Hide SSID
Yes
No
Network Name (SSID)
ASUS Router
Authentication Method
WPA2-Personal
WPA Encryption
AES
WPA Pre-Shared Key
Protected Management Frames
Disable
Group Key Rotation Interval
3600
2.4 GHz
Channel bandwidth
20/40 MHz
Control Channel
AUTO
Current Control Channel: 7
Auto select channel including channel 12, 13
Extension Channel
AUTO
5 GHz-1
Channel bandwidth
20/40/80/160 MHz
Enable 160 MHz
Control Channel
AUTO
Current Control Channel: 60
Auto select channel including DFS channels
Extension Channel
AUTO
5 GHz-2
Channel bandwidth
20/40/80 MHz
Enable 160 MHz
Control Channel
AUTO
Current Control Channel: 100
Auto select channel including DFS channels
Extension Channel
AUTO
6 GHz
Hide SSID
Yes
No
Network Name (SSID)
GT-BE98_6G
Channel bandwidth
20/40/80/160/320 MHz
Control Channel
AUTO
Current Control Channel: 37
enable PSC (Preferred Scanning Channel) to ensure the 6GHz devices connectivity.
Please check FAQ.
Extension Channel
AUTO
Authentication Method
WPA3-Personal
WPA Encryption
AES
WPA Pre-Shared Key
Protected Management Frames
Required
Group Key Rotation Interval
3600
Apply

## 3.16.2 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.

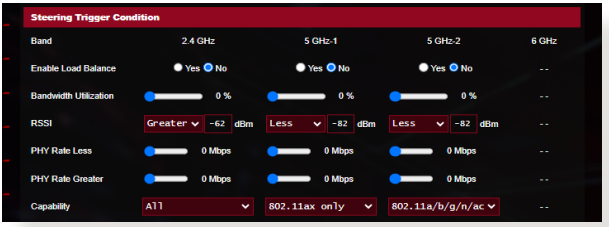



La scheda Regole di Smart Connect è divisa in quattro sezioni:

- 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**

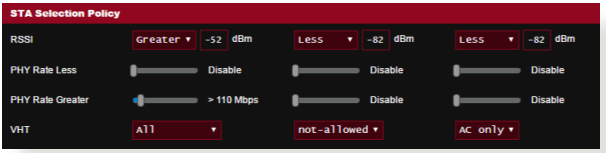
  Se il livello del segnale ricevuto di uno qualsiasi dei client associati soddisfa questa condizione verrà innescato il cambiamento della banda.
- **PHY Rate Less / PHY Rate Greater**

  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.

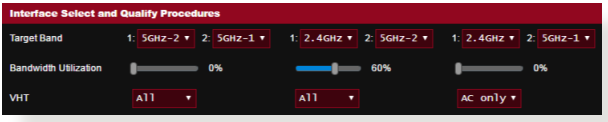
### *Regole di selezione STA*

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




### *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)**.

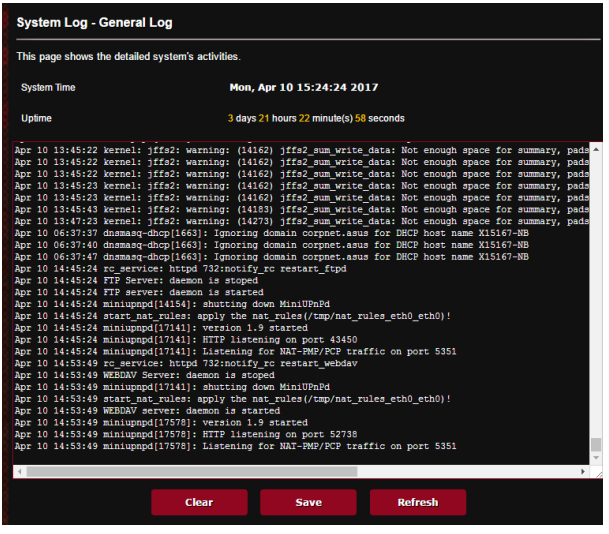
## 3.17 Registro di sistema

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.

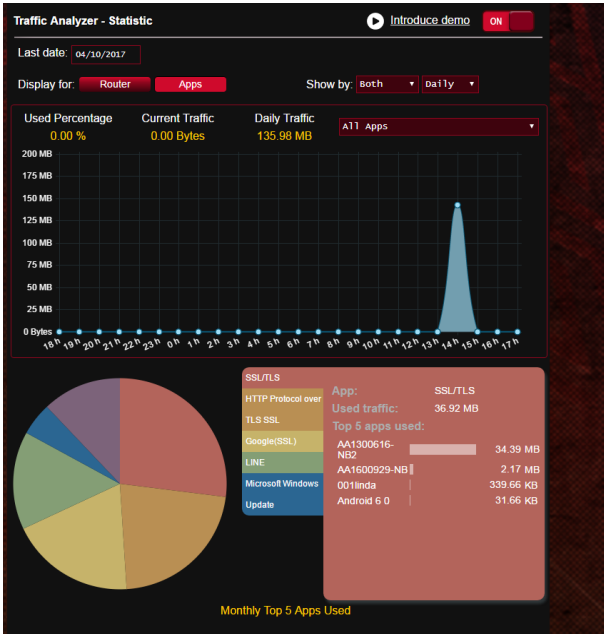
**Per visualizzare il vostro registro di sistema:**

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)
   - Wireless Log (Registro wireless)
   - DHCP Leases (Lease DHCP)
   - IPv6
   - Routing Table (Tabella di routing)
   - Port Forwarding
   - Connessioni



## 3.18 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.



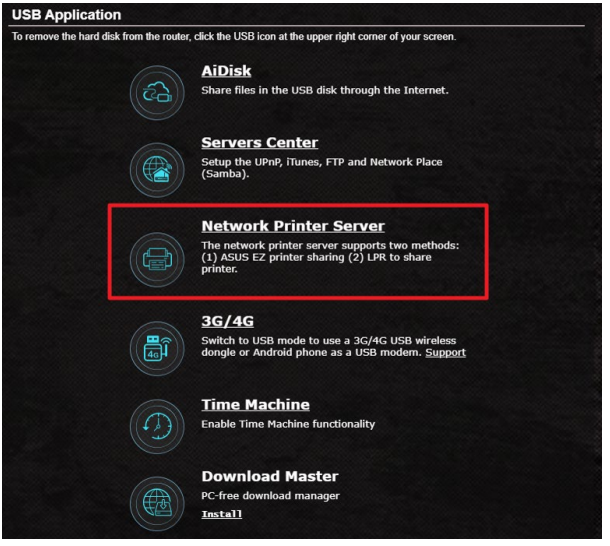

**Per configurare Traffic analyzer:**

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** selezionate la modalità con la quale volete visualizzare le informazioni di traffico.

## 3.19 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 3.0 del pannello posteriore del vostro router wireless. Assicuratevi che il dispositivo di archiviazione USB sia formattato e partizionato correttamente. ate riferimento al sito web ASUS: http://event.asus.com/2009/networks/disksupport/ per ottenere l'elenco dei file system compatibili.

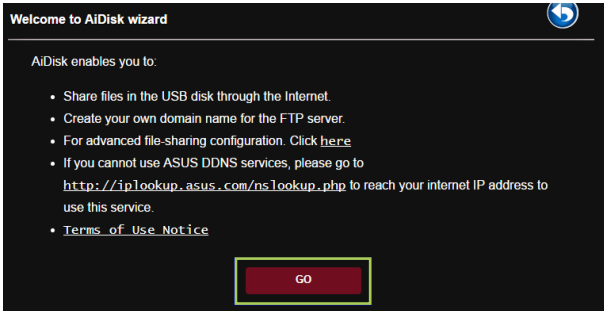


## 3.19.1 Usare AiDisk

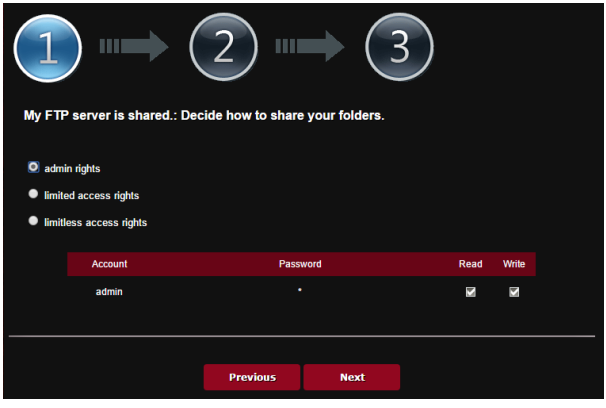
AiDisk vi permette di condividere file memorizzati su un dispositivo USB attraverso la rete Internet. AiDisk, inoltre, vi assiste nella configurazione di ASUS DDNS e del server FTP.

### Per usare AiDisk:

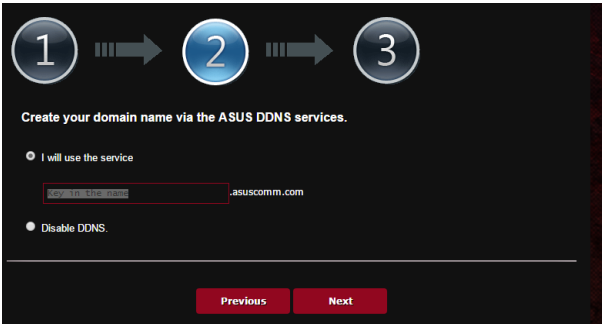
1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate)** > **USB Application (Applicazioni USB)** e poi cliccate sull'icona di **AiDisk**.
2. Nella pagina iniziale di configurazione guidata di AiDisk cliccate su **GO (Vai)**.




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.

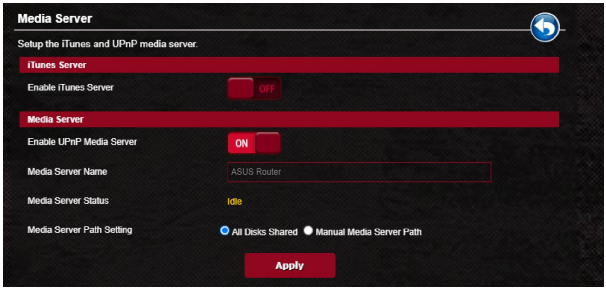
## 3.19.2 Usare Gestione Server

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 UPnP di accedere ai file multimediali presenti sul disco USB collegato al vostro router wireless.

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

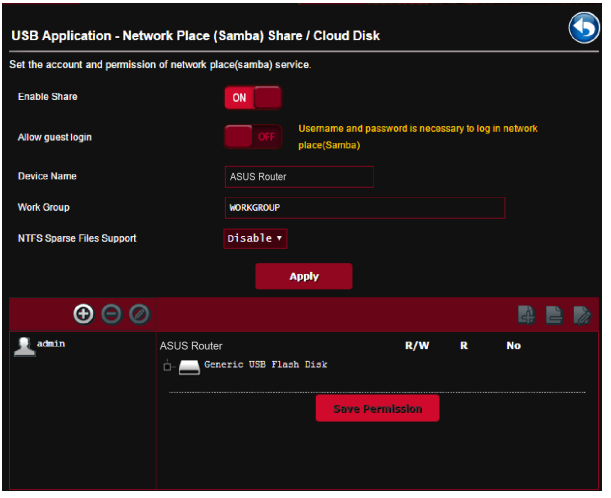



Per lanciare le impostazioni del Server multimediale andate su **Advanced Settings (Impostazioni avanzate)** > **USB Application (Applicazioni USB)** > **Media Servers (Server multimediale)**. Fate riferimento alle seguenti informazioni in merito alle diverse voci presenti nel menu:

- **Enable iTunes Server (Abilitare il server iTunes)?:** Spostate il cursore su ON/OFF per abilitare/disabilitare il Server iTunes.
- **Enable uPnP Media Server (Abilita Server multimediale uPnP):** Spostate il cursore su ON/OFF per abilitare/disabilitare il Server multimediale UPnP.
- **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)** > **Network Place (Samba) Share / Cloud Disk (Condivisione Risorse di rete (Samba) / Disco Cloud)**.

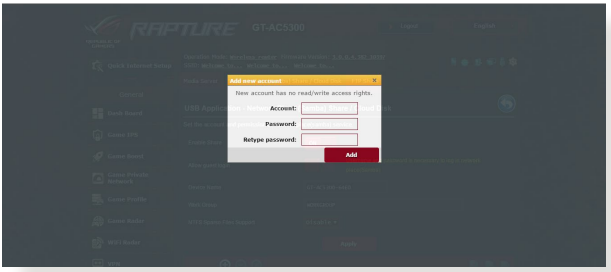
   **NOTA:** Condivisione Samba, per la rete locale, è abilitata di default.

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.

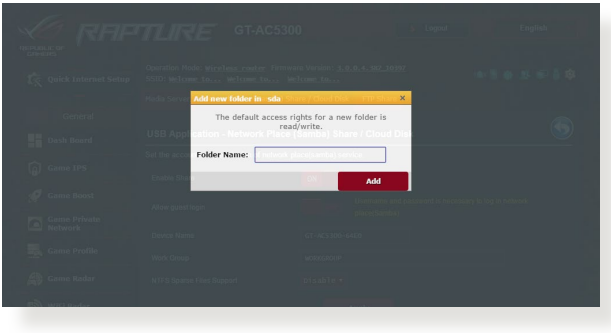
b) Cliccate su .

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.



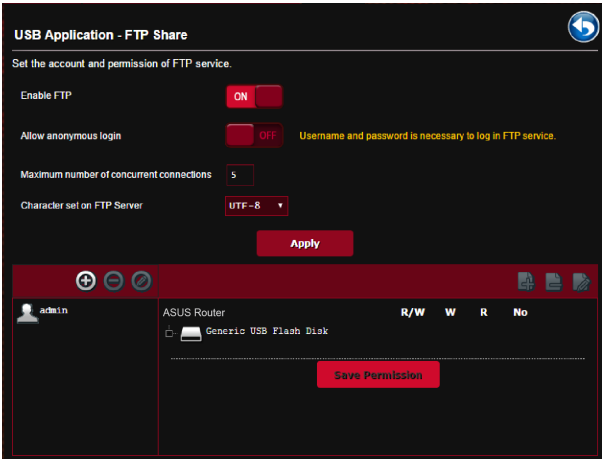

3. Nell'elenco delle cartelle selezionate i permessi di accesso che volete assegnare alle cartelle specifiche:
   - **R/W**: Selezionate per impostare i permessi di lettura (R) e scrittura (W).
   - **R**: Selezionate per impostare i permessi di sola lettura.
   - **No**: Selezionate questa opzione se 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 *3.13.3 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 *3.19.1 Usare AiDisk*.

1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate)** > **USB Application (Applicazioni USB)** > **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.
   - **W**: 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.

### 3.19.3 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.

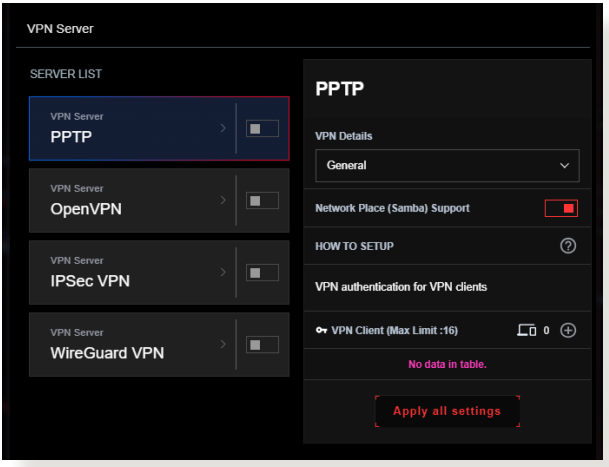
   - **Username / Password (Nome utente / Password):** Il **nome utente** e la **password** sono fornite dal vostro operatore 3G/4G.
   - **Modem USB:** Scegliete il modello del vostro modem USB 3G/4G dall'elenco a disposizione. Se non siete sicuri del modello selezionate **Auto (Automatico)**.
4. Cliccate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

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

## 3.20 VPN

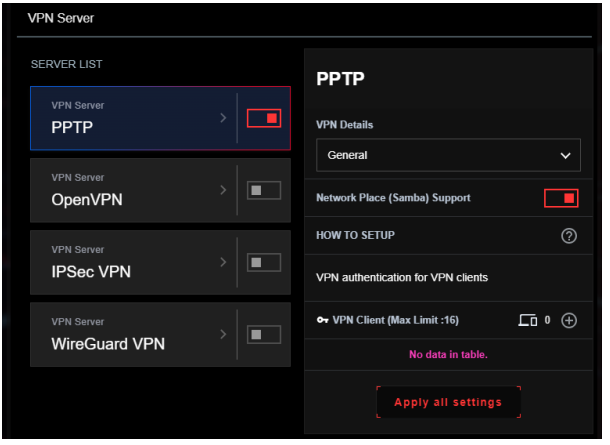
Il servizio VPN (Virtual Private Network) instaura un canale di comunicazione sicura con un computer, o una rete, remoti usando l'infrastruttura pubblica della rete Internet.

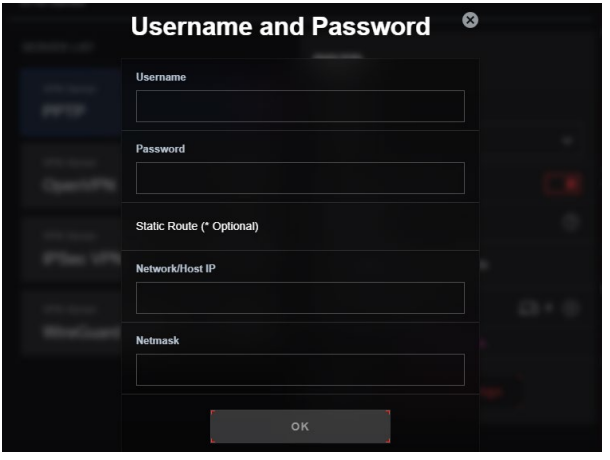
**NOTA:** Prima di impostare una connessione VPN avrete bisogno di un indirizzo IP (o un nome del dominio) del server VPN.



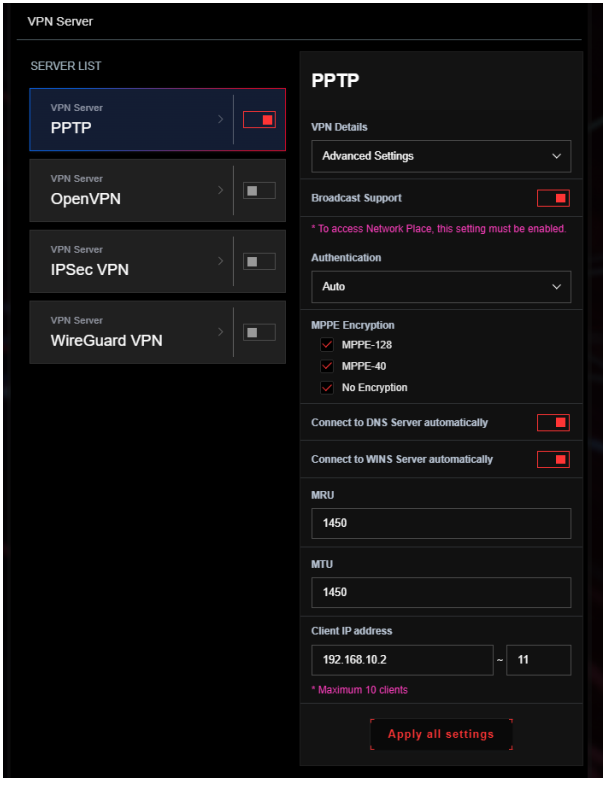

**Per configurare l'accesso ad un server VPN:**

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 **General (Generale)** e attivare Network Place (Samba) Support (Supporto risorsa di rete (Samba)).
4. Fare clic su ⊕ per aggiungere un client VPN e immettere nome utente e password per l'accesso VPN.


VPN Server
SERVER LIST
VPN Server
PPTP
VPN Server
OpenVPN
VPN Server
IPSec VPN
VPN Server
WireGuard VPN
PPTP
VPN Details
General
Network Place (Samba) Support
HOW TO SETUP
VPN authentication for VPN clients
VPN Client (Max Limit :16)
0
No data in table.
Apply all settings

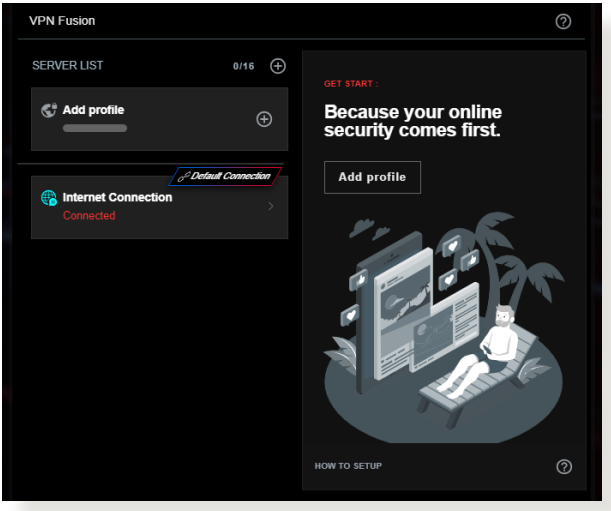

Username and Password
Username
Password
Static Route (* Optional)
Network/Host IP
Netmask
OK

5. 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.
6. Cliccate su **Applica tutte le impostazioni**.



### 3.20.1 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:**

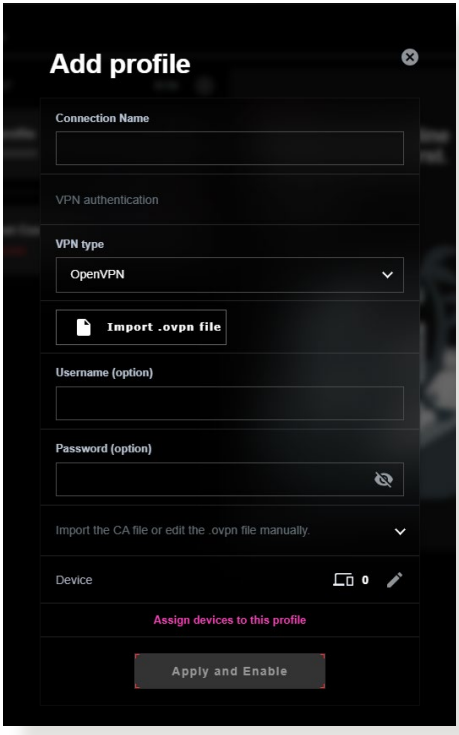
1. Dal pannello di navigazione andate su **General (Generale)** > **VPN** > **VPN Fusion (Fusione VPN)** e fare clic su ⊕ per creare un nuovo profilo.
2. Selezionare **PPTP** nell'elenco a discesa **VPN type (Tipo VPN)** per creare un profilo client VPN.

**IMPORTANTE!** Il server VPN e il client VPN devono essere dello stesso tipo VPN.

3. Immettere le informazioni sul server VPN nel client VPN.
   (1) **Nome connessione:** Personalizzare un nome per rappresentare questo profilo.
   (2) **Server VPN:** Immettere l'indirizzo IP o il nome DDNS del server VPN.
   (3) **Nome utente:** Immettere le informazioni fornite dal server VPN.
   **Password:** Immettere le informazioni fornite dal server VPN.
   (4) Fare clic su **Apply and Enable (Applica e Abilita)** per completare il profilo client VPN e connettersi al server VPN.

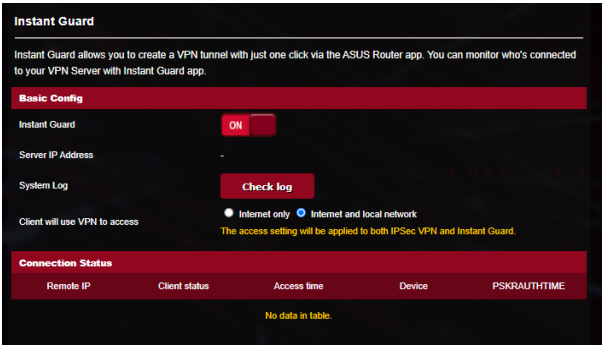
**NOTA:** Contattare l'amministratore del server VPN per le informazioni sul server VPN.

4. Quando viene visualizzato **Connected (Connesso)**, la connessione VPN PPTP è stata configurata correttamente.



## 3.20.2 Instant Guard (Protezione immediata)

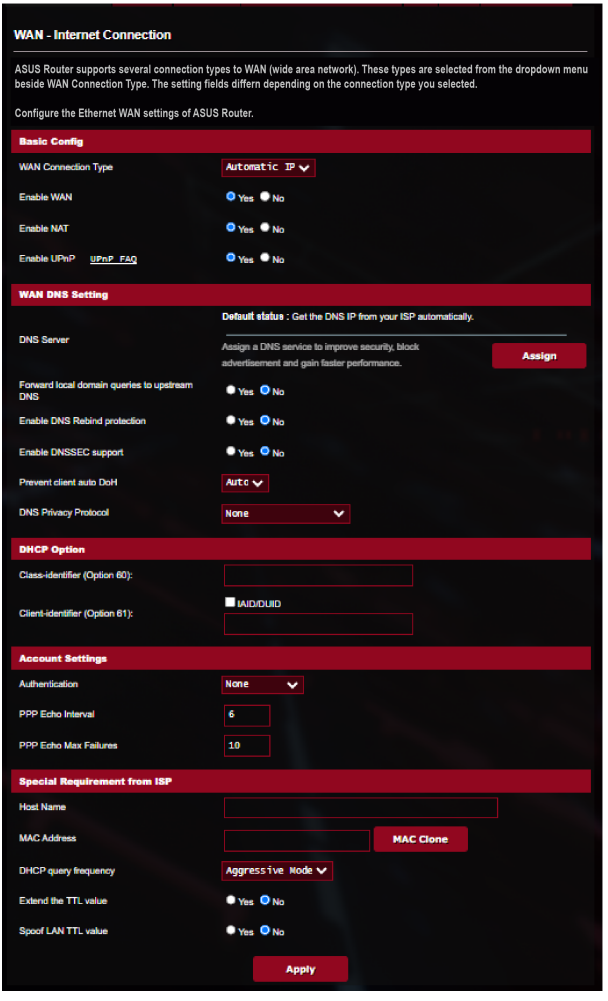
Instant Guard (Protezione immediata) esegue il server VPN privato sul router. Quando si utilizza un tunnel VPN, tutti i dati passano attraverso il server. Con Instant Guard (Protezione immediata), si è in controllo totale del proprio server, rendendolo la soluzione più sicura.



# 3.21 WAN

## 3.21.1 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** > **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

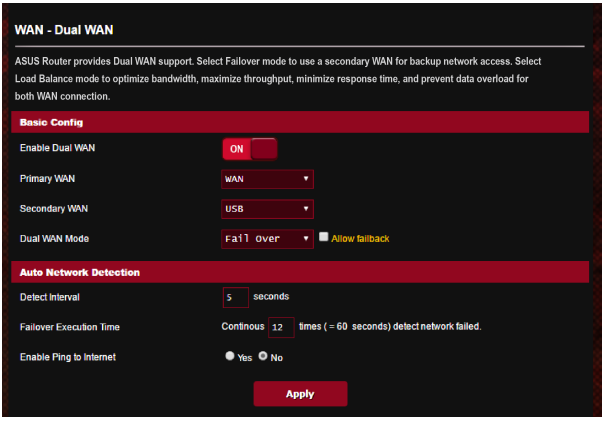
volta collegati in rete i dispositivi possono essere configurati da remoto per supportare applicazioni P2P (peer-to-peer), gioco online, video conferenze e server proxy o web. A differenza del Port Forwarding, il quale richiede la configurazione manuale delle porte, UPnP configura automaticamente il 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.

## 3.21.2 WAN duale

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

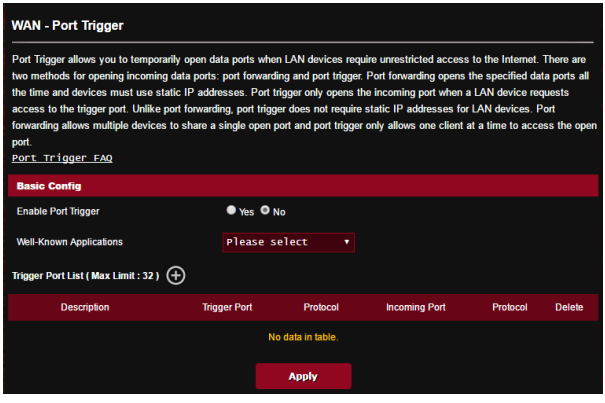
- **Modalità failover:** Selezionate questa modalità per usare la WAN secondaria come accesso di riserva alla rete.
- **Modalità bilanciata:** Selezionate questa modalità per ottimizzare la banda, minimizzare il tempo di risposta e prevenire sovraccarico di dati per ciascuna delle due WAN.



## 3.21.3 Port Trigger

Il trigger di un intervallo di porte apre una porta in ingresso predeterminata 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** > **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 Tigger.
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.

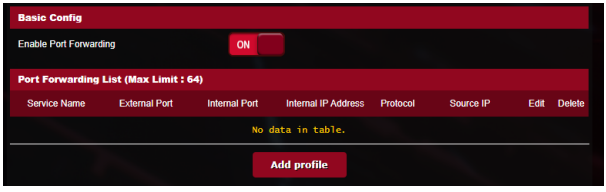
5. Cliccate sul pulsante **Add (Aggiungi)** per inserire le informazioni per la porta trigger nell'elenco. Cliccate sul pulsante **Delete (Elimina)** per rimuovere una porta trigger dall'elenco.
6. Quando avete finito cliccate su **Apply (Applica)**.

**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.

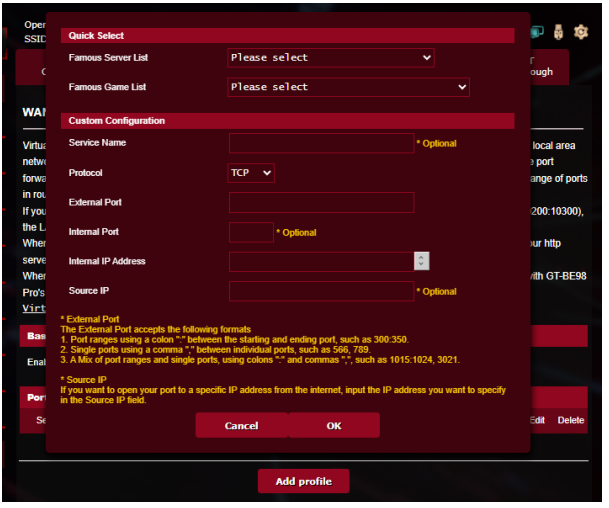
## 3.21.4 Virtual Server/Port Forwarding

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** > **Virtual Server / Port Forwarding**.
2. Selezionate **ON** alla voce **Enable Port Forwarding (Abilita Port Forwarding)**.
3. Fare clic su **Add profile (Aggiungi profilo)**.




4. Nel campo **Famous Server List (Servizi più comuni)** selezionate il tipo di servizio al quale volete accedere.
5. 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.
6. 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 *3.12 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)**.

7. 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.
8. 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 dovreste 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.

### 3.21.5 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** > **DMZ**.
2. Configurate le seguenti impostazioni. Quando avete finito cliccate su **Apply (Applica)**.

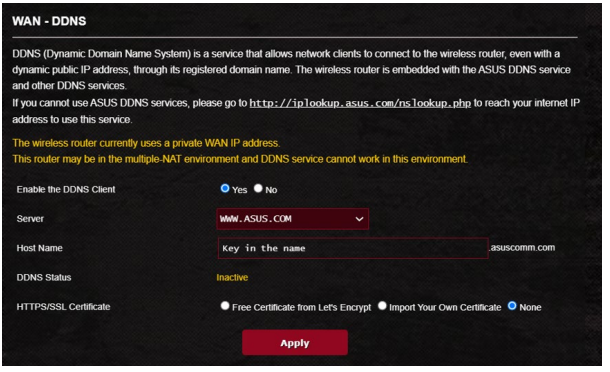
- **Indirizzo IP del client bersaglio:** Inserite l'indirizzo IP (relativo alla rete locale) del client per il quale volete attivare il servizio DMZ in modo da esporlo alla rete Internet. Assicuratevi che il client disponga di un indirizzo IP statico.

**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)**.

## 3.21.6 DDNS

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** > **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:**

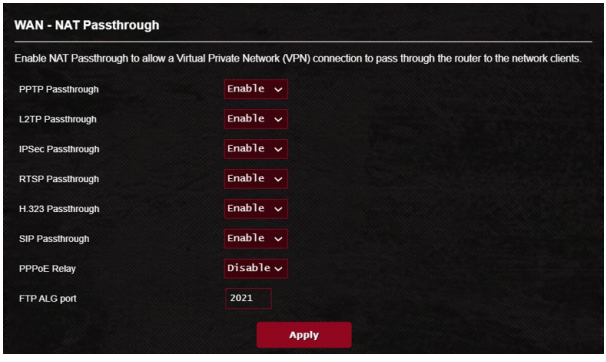
Il server DNS Dinamico non funzionerà nei seguenti casi:

- 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.

## 3.21.7 NAT Passthrough

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

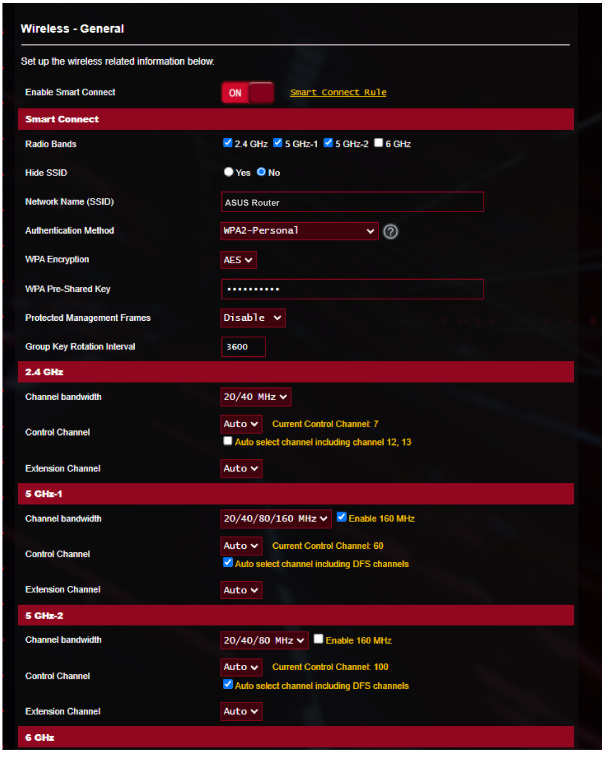
Per abilitare / disabilitare le funzionalità NAT Passthrough andate su **Advanced Settings (Opzioni avanzate)** > **WAN** > **NAT Passthrough**. Quando avete finito cliccate su **Apply (Applica)**.



# 3.22 Wireless

## 3.22.1 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** > **General (Generale)**.
2. Selezionate 2.4GHz, 5GHz-1, 5GHz-2 o 6GHz 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 client della vostra rete alla banda più appropriata (2.4GHz, 5GHz-1, 5GHz-2 o 6GHz) 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.

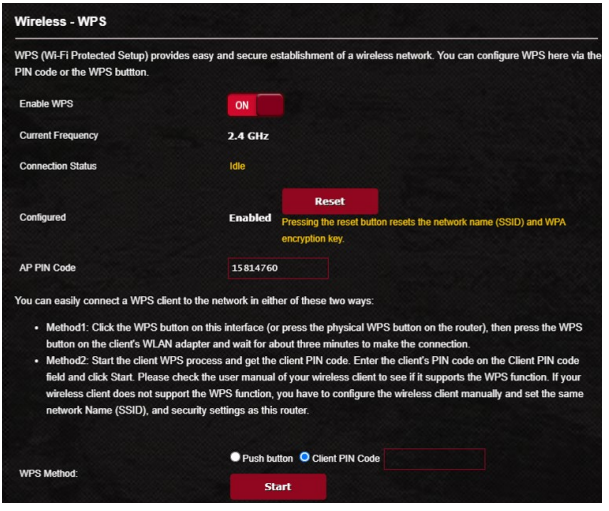
   **NOTA:** Potete assegnare solo un SSID per entrambe le bande di frequenza 2.4 GHz, 5GHz-1, 5GHz-2 e 6GHz.

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)**.

## 3.22.2 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** > **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/WPA2/WPA3-Personal. WPS non supporta una rete wireless che usa una metodi di cifratura a chiave condivisa, WPA/WPA2/WPA3-Enterprise e RADIUS.

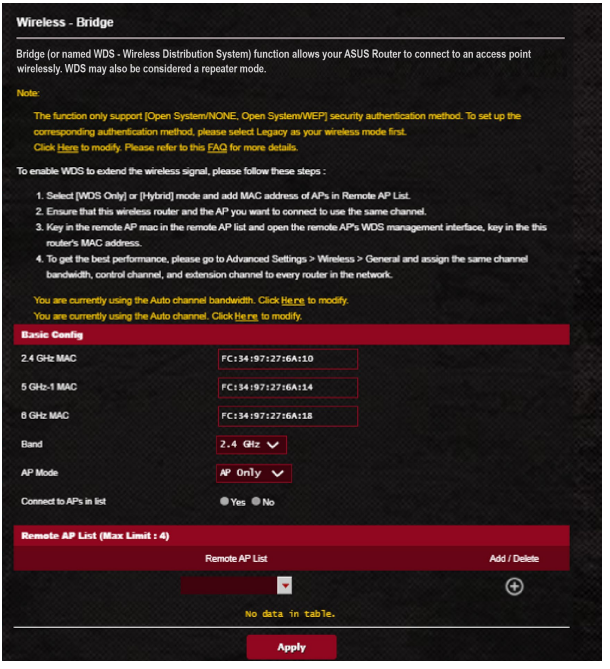
4. Nel campo **WPS Method (Modalità WPS)** selezionate **Push Button (Premi Pulsante)** o **Client PIN code (Codice PIN client)**. Se selezionate **Push Button (Premi Pulsante)** andate al passaggio 5. Se selezionate **Client PIN code (Codice PIN client)** andate al passaggio 6.
5. Per impostare il WPS 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.

## 3.22.3 WDS

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** > **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 WDS):** 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.

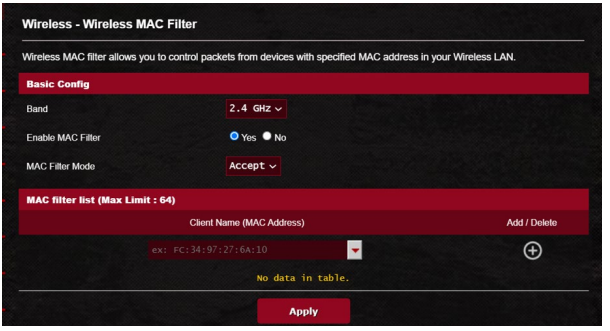
6. In **Elenco AP remoti** inserite un indirizzo MAC e cliccate sul pulsante **Add (Aggiungi)** ⊕ per inserire l'indirizzo MAC di altri Access Point disponibili.

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

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

## 3.22.4 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.

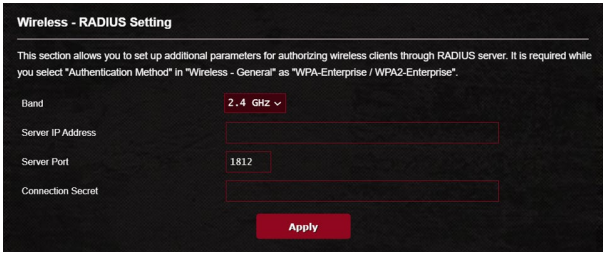



**Per impostare il Filtro MAC wireless:**

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

## 3.22.5 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/WPA2/WPA3-Enterprise o 802.1be.




**Per configurare le impostazioni wireless RADIUS:**

1. Assicuratevi che la modalità di autenticazione wireless del router sia impostata su WPA/WPA2/WPA3-Enterprise.

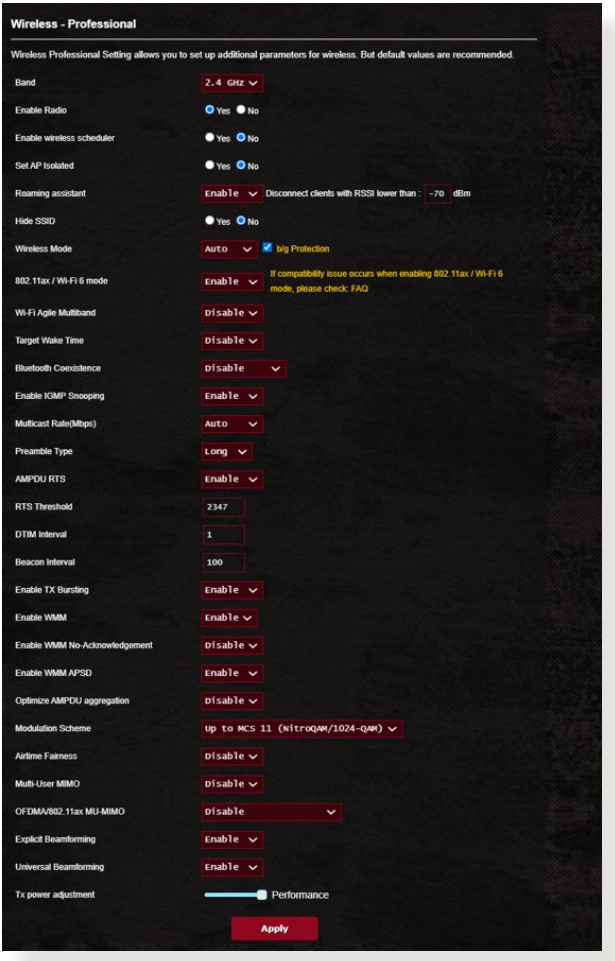
   **NOTA:** Fate riferimento alla sezione *3.22.1 Generale* per la configurazione della modalità di autenticazione del vostro router wireless.

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)**.

## 3.22.6 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:

- **Band:** Selezionate la banda di frequenza.

- **Enable Radio (Abilita WiFi):** Selezionate **Yes (Sì)** per abilitare la rete wireless. Selezionate **No** per disabilitarla.
- **Enable wireless scheduler (Abilita programmatore wireless):** Selezionare **Yes (Sì)** per abilitare e configurare il programmatore wireless. Selezionare **No** per disabilitare il programmatore wireless.
  - **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 è il periodo di tempo che passa tra due segnali DTIM consecutivi. Il valore standard è di 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.
- **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 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.

## 4.1 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.

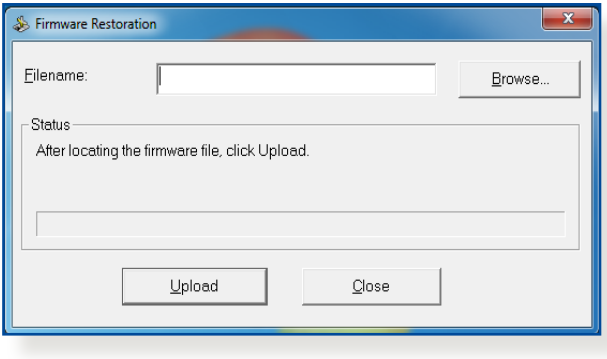
**Per lanciare l'utility Device Discovery:**

- 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.

## 4.2 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**: 192.168.50.1

   **Maschera di sottorete**: 255.255.255.0
4. Dal desktop cliccate su **Start** > **Tutti i programmi** > **ASUS Utility GT-BE98 Wireless Router** > **Firmware Restoration**.

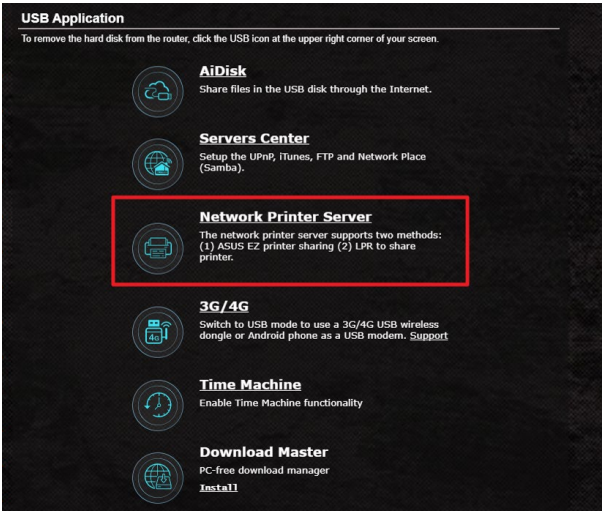
5. Selezionate il file specifico e poi cliccate su **Upload (Carica)**.

**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 3*: *Configurare le impostazioni generali e avanzate per maggiori dettagli.*

## 4.3 Impostare il server di stampa

### 4.3.1 ASUS EZ Printer Sharing

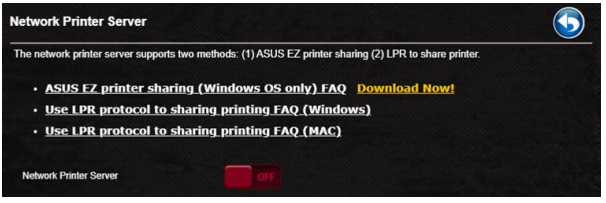
ASUS EZ Printer Sharing vi permette di connettere una stampante USB alla porta USB del vostro router wireless e creare un server di stampa. In questo modo i client della vostra rete possono stampare file o fare scansioni di documenti senza bisogno di cavi.



**NOTA:** Le funzioni del server di stampa sono supportate su Windows® 10/11.

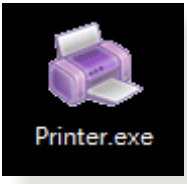
**Per configurare la modalità condivisione stampante EZ:**

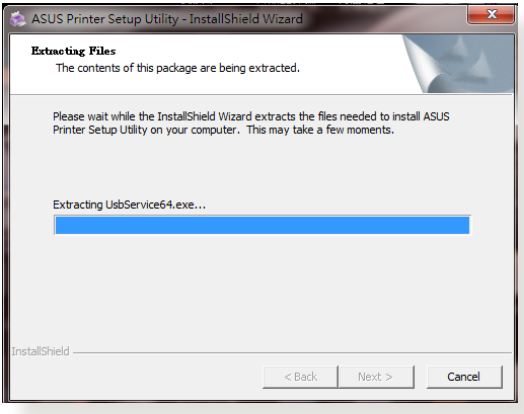
1. Dal pannello di navigazione andate su **Advanced Settings (Impostazioni avanzate)** > **USB Application (Applicazioni USB)** > **Network Printer Server (Server di stampa di rete)**.
2. Cliccate su **Download Now (Scarica Adesso)** per scaricare l'utility per la stampante di rete.



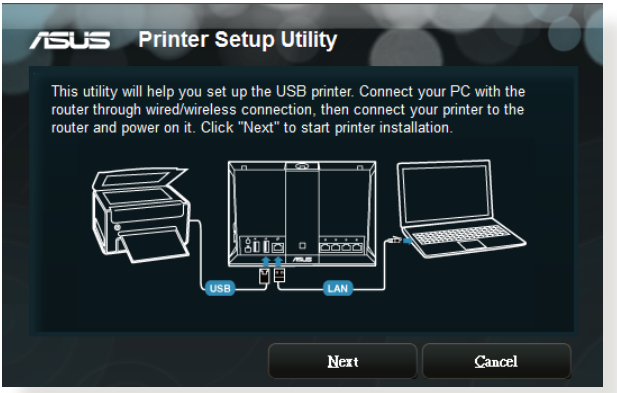

**NOTA:** L'utility per le stampanti di rete è supportata su Windows® 10/11. Per installare l'utility su Mac OS selezionate **Use LPR protocol for sharing printer (Usa il protocollo LPR per condividere la stampante)**.

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



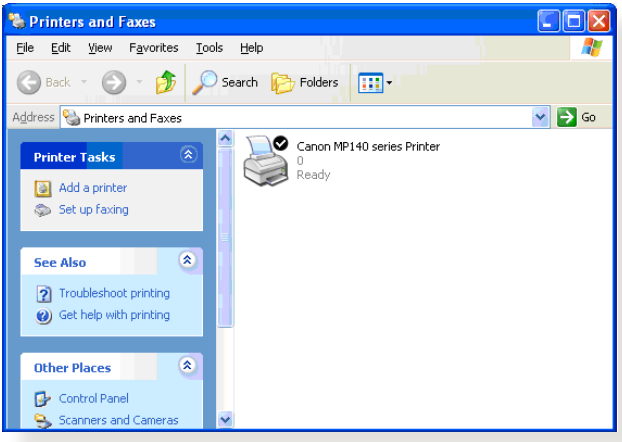
4. Seguite le istruzioni sullo schermo per completare il processo di installazione dell'hardware e poi cliccate su **Next (Avanti)**.




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.



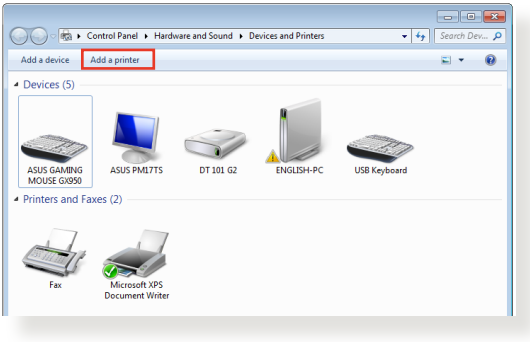
### 4.3.2 Utilizzo di LPR per condividere una stampante

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

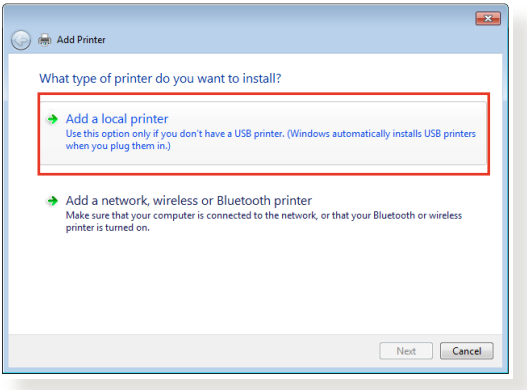
#### Condividere la vostra stampante LPR

**Per condividere la vostra stampante LPR:**

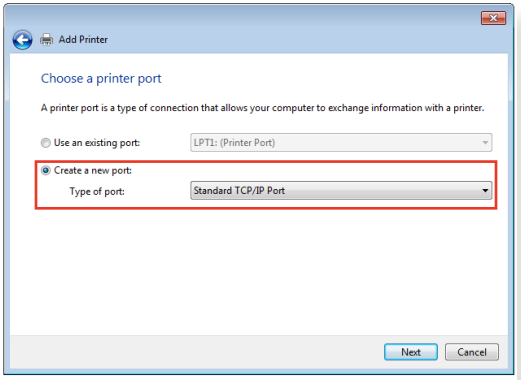
1. Dal Desktop di Windows® cliccate su **Start** > **Devices and Printers (Dispositivi e Stampanti)** > **Add a printer (Aggiungi stampante)** per far partire la procedura guidata **Add Printer Wizard (Aggiungi stampante)**.



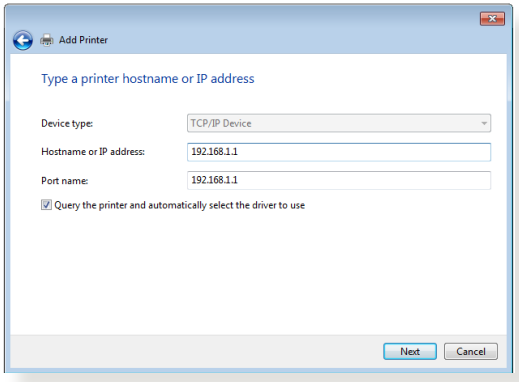

2. Selezionate **Add a local printer (Aggiungi stampante locale)** e poi cliccate su **Next (Avanti)**.



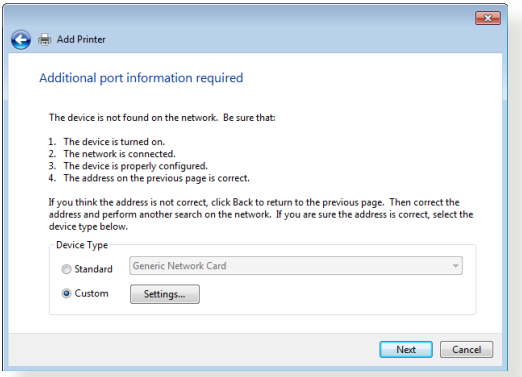
3. Selezionate **Create a new port (Crea una nuova porta)** e poi impostate il tipo **Standard TCP/IP Port** nel campo **Type of Port (Tipo di porta)**. Cliccate su **Next (Avanti)**.



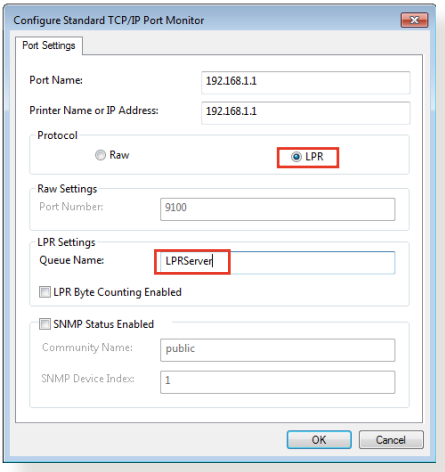

4. Nel campo **Hostname or IP address (Nome host o indirizzo IP)** inserite l'indirizzo IP del router wireless e poi cliccate su **Next (Avanti)**.



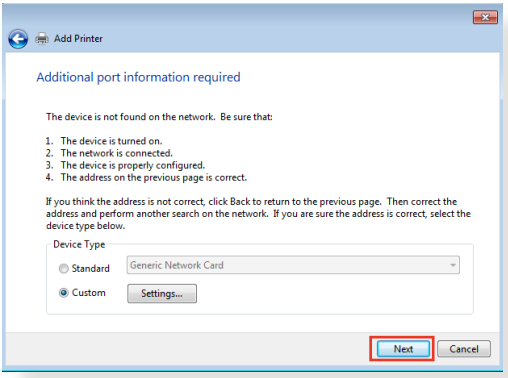
5. Selezionate **Custom (Personalizzata)** e poi cliccate su **Impostazioni**.



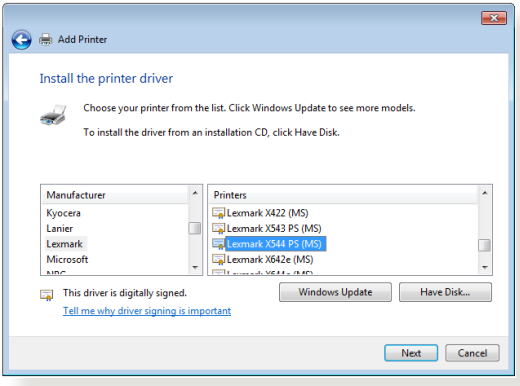

6. Impostate il **Protocol (Protocollo)** su **LPR**. Nel campo **Queue Name (Nome coda)** inserite **LPRServer** e poi cliccate su **OK** per continuare.



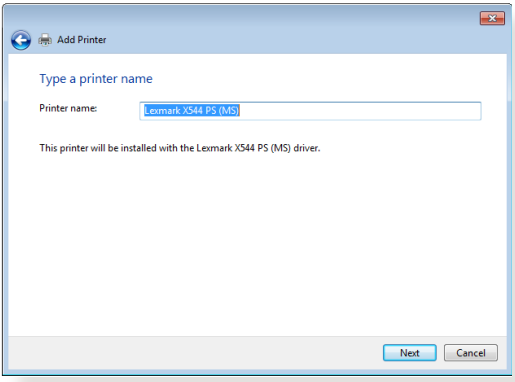
7. Cliccate su **Next (Avanti)** per completare le impostazioni della porta TCP/IP standard.



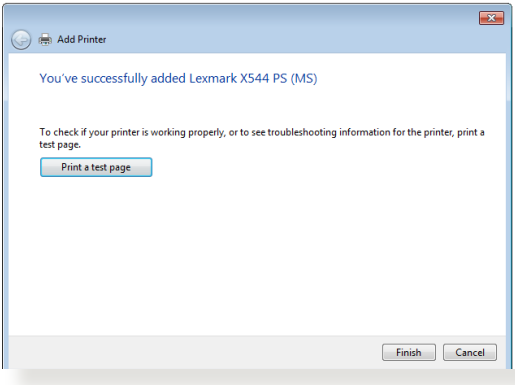

8. Installate i driver della stampante selezionando il produttore e il modello corretti dall'elenco. Se la vostra stampante non è nell'elenco cliccate su **Have Disk (Disco driver...)** per installare i driver da un supporto CD-ROM o da un file manualmente.



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




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



## 4.4 Download Master

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

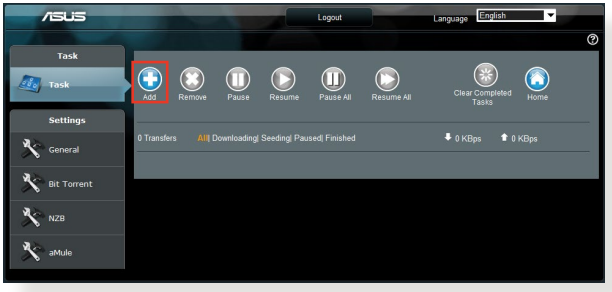
**NOTA:** Per utilizzare Download Master avete bisogno di un dispositivo di archiviazione USB connesso al router wireless.

**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.

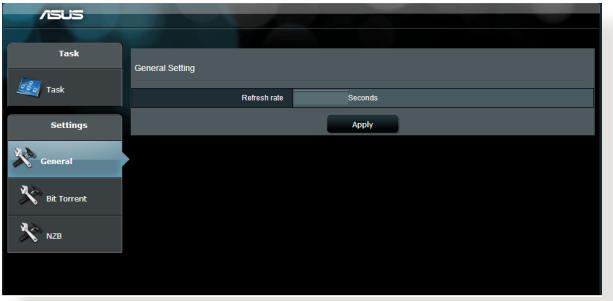
2. Quando il download è completato cliccate sull'icona di Download Master per iniziare ad usare l'applicazione.
3. Cliccate su **Add (Aggiungi)** per aggiungere un download.



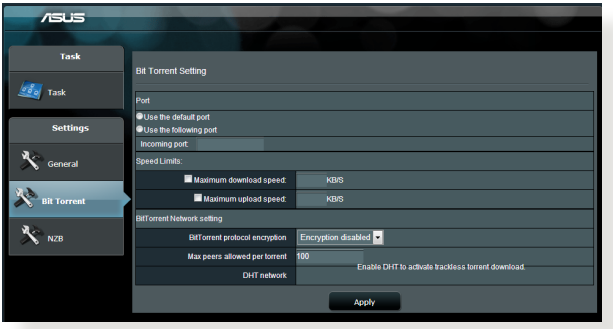

4. Selezionate un protocollo di download come Torrent, HTTP o FTP. Se necessario fornite un file .torrent, o un magnet link, per iniziare il download.

   **NOTA:** Per maggiori dettagli fate riferimento alla sezione *4.4.1 Impostazioni Torrent*.

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




## 4.4.1 Impostazioni Torrent

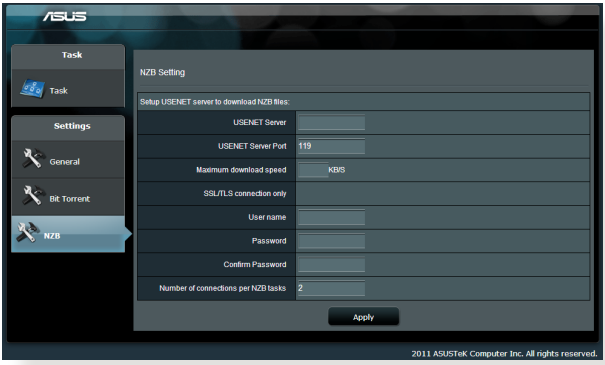



**Per configurare le impostazioni di download tramite Torrent:**

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.

## 4.4.2 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)**.



# 5 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.

## 5.1 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)** > **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://rog.asus.com/networking/rog-rapture-gt-be98-model/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.

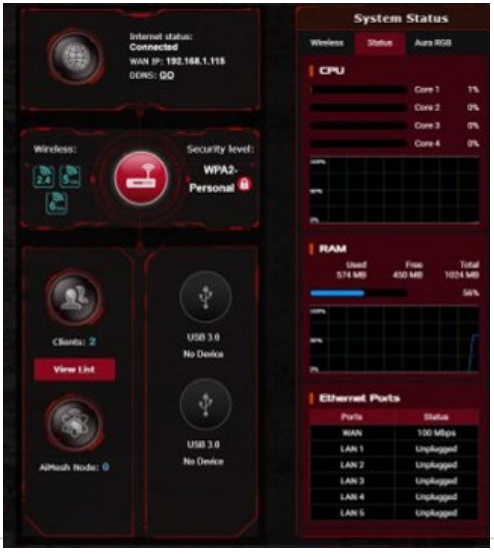
- Quando il cavo Ethernet che connette il router al modem è collegato correttamente il LED WAN sul router è acceso.
- Quando il cavo Ethernet che connette il vostro computer (acceso) al router è collegato correttamente il LED LAN corrispondente sul router è acceso.

### 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.

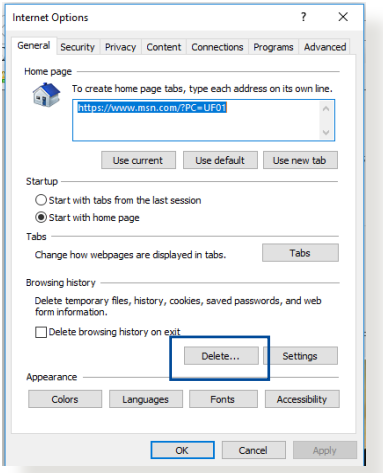
- Ogni client sulla rete deve avere un indirizzo IP valido. ASUS raccomanda di usare il server DHCP del router wireless per assegnare automaticamente gli indirizzi IP ai computer della vostra rete.
- Alcuni fornitori di connessione dati via cavo potrebbero richiedere che l'indirizzo MAC del vostro computer 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.



## 5.2 Domande e risposte 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 la procedura standard per rimuovere i cookie e i file temporanei è la seguente:




  1. Lanciate Internet Explorer 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**.

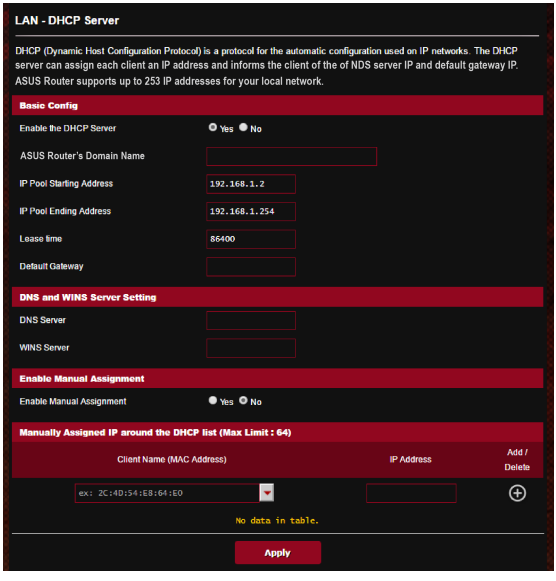
**NOTE:**

- 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.

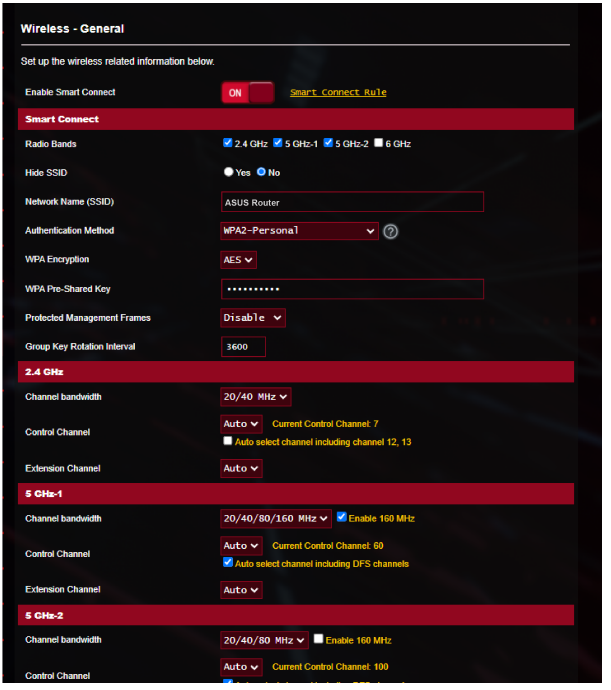
## Il client non riesce a stabilire una connessione wireless con il router.

**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.

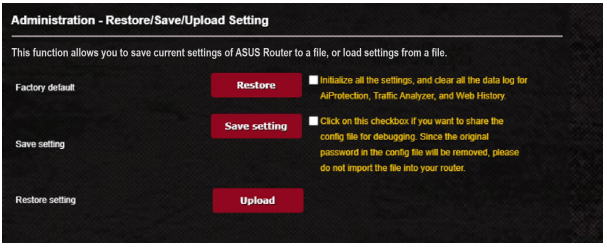
- **Fuori portata:**
  - Avvicinate il router al client wireless.
  - Provate a modificare l'angolazione delle antenne del router per trovare la direzione migliore come descritto nella sezione *1.4 Posizionamento* del router.
- **Il server DHCP è stato disabilitato:**
  1. Aprite l'interfaccia web. Andate 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)** > **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 chiave 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:

  **Nome utente:** admin

  **Password:** admin

  **Abilita Server DHCP:** Sì (se il cavo WAN è collegato)

  **Indirizzo IP:** http://www.asusrouter.com (o 192.168.50.1)

  **Nome dominio:** (Vuoto)

  **Maschera di sottorete:** 255.255.255.0

  **Server DNS primario:** 192.168.50.1

  **Server DNS secondario:** (Vuoto)

  **SSID (2.4GHz):** ASUS_XX_2G

  **SSID (5GHz-1):** ASUS_XX_5G-1

  **SSID (5GHz-2):** ASUS_XX_5G-2

  **SSID (6GHz):** ASUS_XX_6G

## Aggiornamento del firmware non riuscito.

Lanciate la modalità di recupero e eseguite l'utility Firmware Restoration. Fate riferimento alla sezione *4.2 Firmware Restoration* per avere maggiori informazioni su come effettuare il recupero del firmware.

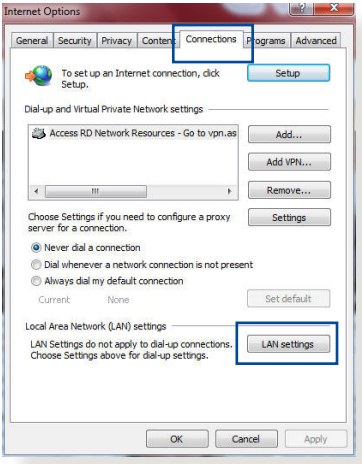
## Impossibile accedere all'interfaccia web

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.

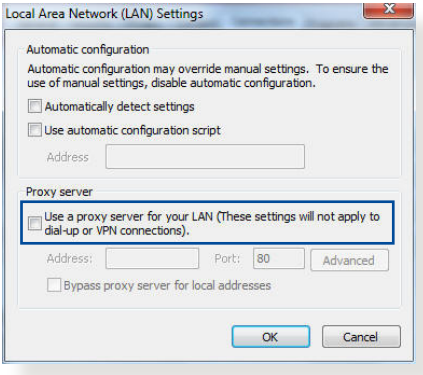
### A. Disabilitate il server proxy (se abilitato).

#### Windows®

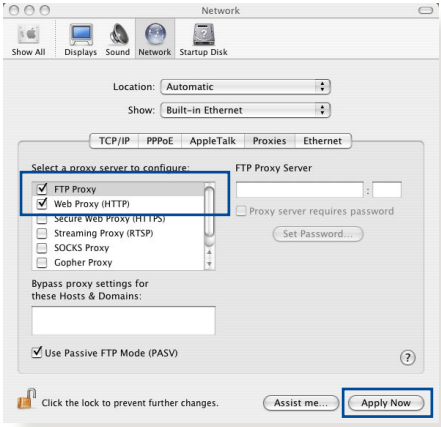
1. Cliccate su **Start** > **Internet Explorer** per aprire il browser.
2. Cliccate su **Tools (Strumenti)** > **Internet options (Opzioni Internet)** > **Connections (Connessioni)** e cliccate su **LAN settings (Impostazioni LAN)**.




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



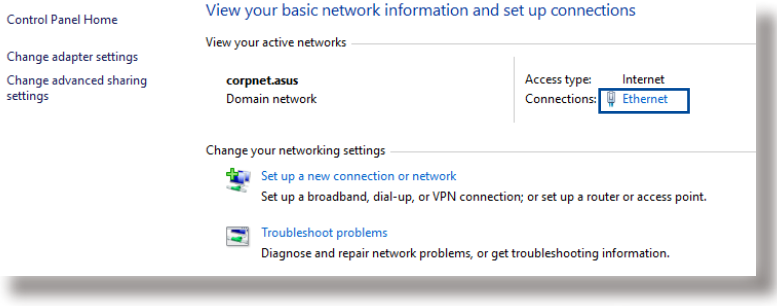

1. Dal vostro browser Safari cliccate su **Safari** > **Preferences (Preferenze)** > **Advanced (Avanzate)** > **Change Settings (Modifica Impostazioni)**.
2. Dal pannello **Network** togliete la spunta da **FTP Proxy (Proxy FTP)** e **Web Proxy (HTTP) (Proxy web (HTTP))**.
3. Quando avete finito selezionate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

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

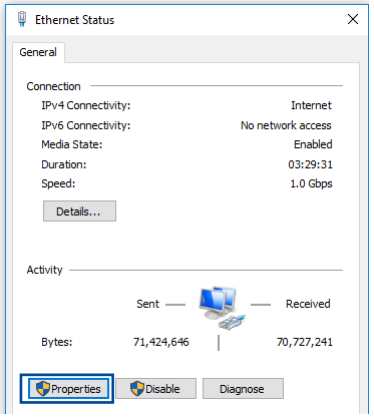
## B. Configurate le impostazioni TCP/IP in modo da ottenere un indirizzo IP automaticamente.

### Windows®

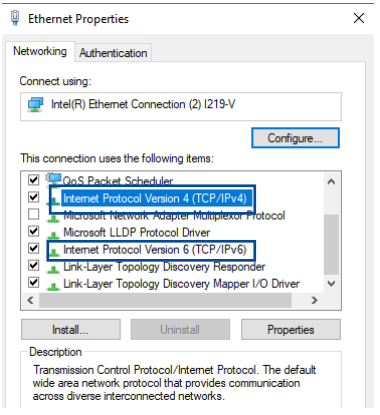
1. Cliccate su **Start** > **Control Panel (Pannello di controllo)** > **Network and Sharing Center (Centro connessioni di rete e condivisione)** quindi cliccate sulla connessione di rete per visualizzare la finestra di stato.



2. Cliccate su **Properties (Proprietà)** per visualizzare la finestra delle proprietà Ethernet.



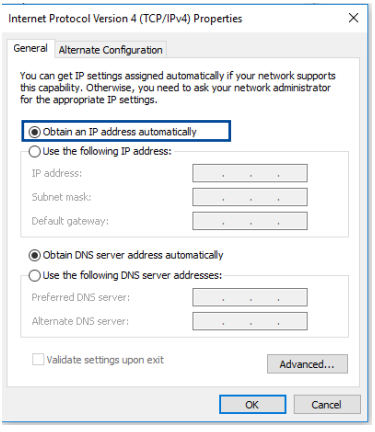

3. Selezionate **Protocollo Internet versione 4 (TCP/IPv4)** o **Internet Protocol Version 6 (TCP/IPv6) (Protocollo Internet versione 6 (TCP/IPv6))** e poi cliccate su Proprietà.



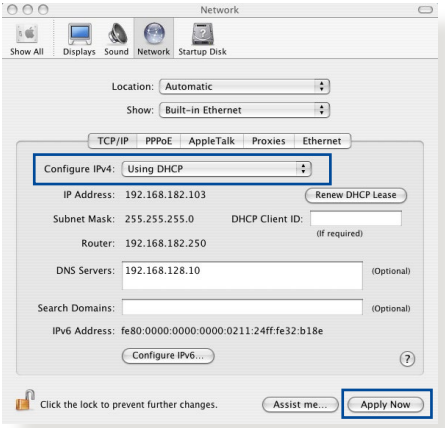

4. Per ottenere automaticamente le impostazioni IPv4 selezionate **Ottieni automaticamente un indirizzo IP**.

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

5. Quando avete finito selezionate **OK**.



## MAC OS

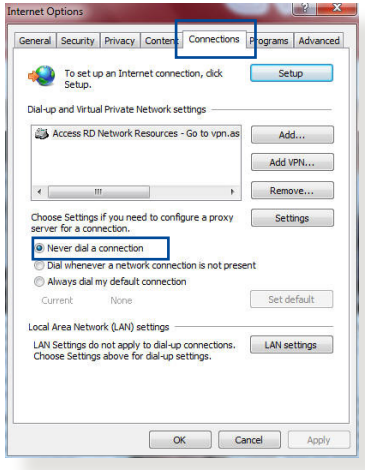



1. Cliccate sull'icona della mela  sulla parte in alto a destra del vostro schermo.
2. Cliccate su **System Preferences (Preferenze di Sistema)** > **Network (Rete)** > **Configure... (Configura...)**.
3. Dal pannello **TCP/IP** selezionate **Using DHCP (Utilizzo di DHCP)** nell'elenco **Configure IPv4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




1. Cliccate su **Start** > **Internet Explorer** per aprire il browser.
2. Cliccate su **Tools (Strumenti)** > **Internet options (Opzioni Internet)** > **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

## GNU General Public License

### Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please see The GNU General Public License for the exact terms and conditions of this license. All future firmware updates will also be accompanied with their respective source code. Please visit our web site for updated information. Note that we do not offer direct support for the distribution.

**GNU GENERAL PUBLIC LICENSE**

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

### Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

## Terms & conditions for copying, distribution, & modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License.

Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide

if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.

    For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

## NO WARRANTY

11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

# Comunicazioni sulla sicurezza

Quando si utilizza questo prodotto, seguire sempre le precauzioni fondamentali di sicurezza, incluso, a titolo esemplificativo ma non esaustivo, quanto segue:

**AVVERTIMENTO!**

- Il cavo o i cavi di alimentazione devono essere inseriti a prese che sono dotate di un'adeguata messa a terra. Collegare l'apparecchio solo ad una presa vicina e facilmente accessibile.
- Se l'adattatore è danneggiato non provare a ripararlo. Contattate un tecnico qualificato o il vostro rivenditore.
- NON utilizzare cavi di alimentazione, accessori o periferiche danneggiate.
- NON montate questo dispositivo ad un'altezza superiore a 2 metri.
- Usa questo prodotto in ambienti la cui temperatura sia compresa tra 0°C(32°F) e 40°C(104°F).
- Leggere le linee guida per l'uso e l'intervallo di temperature forniti prima di utilizzare il prodotto.
- Prestare particolare attenzione alla sicurezza personale quando si utilizza questo dispositivo in aeroporti, ospedali, stazioni di servizio e officine professionali.
- Interferenza del dispositivo medico: Mantenere una distanza minima di almeno 15 cm (6 pollici) tra i dispositivi medici impiantati e i prodotti ASUS per ridurre il rischio di interferenze.
- Utilizzare i prodotti ASUS in buone condizioni di ricezione per ridurre al minimo il livello di radiazioni.
- Tenere il dispositivo lontano dalla portata delle donne incinte e dal basso addome degli adolescenti.
- NON utilizzare questo prodotto se si possono osservare difetti visibili o se è stato bagnato, danneggiato o modificato. Richiedere assistenza.

**AVVERTIMENTO!**

- Non collocare il dispositivo su superfici irregolari o instabili.
- NON posizionare o far cadere oggetti sopra il prodotto. Evitare di esporre il prodotto a urti meccanici quali schiacciamento, piegatura, foratura o frantumazione.
- NON smontare, aprire, mettere nel microonde, incenerire, dipingere o inserire oggetti estranei in questo prodotto.
- Consulta l'etichetta indicante la potenza posta sul fondo del prodotto e assicurati che l'adattatore di alimentazione sia compatibile con tali valori.
- Tenere il prodotto lontano dal fuoco e da fonti di calore.
- NON esporre a liquidi, pioggia o umidità. NON utilizzare il prodotto durante i temporali.
- Collegare i circuiti di uscita PoE di questo prodotto esclusivamente alle reti PoE, senza indirizzarli a strutture esterne.
- Per prevenire il rischio di scosse elettriche scollega il cavo di alimentazione dalla presa di corrente prima di spostare il sistema.
- Utilizzare solo accessori approvati dal produttore del dispositivo per funzionare con questo modello. L'uso di altri tipi di accessori potrebbe invalidare la garanzia o violare le normative e le leggi locali e potrebbe comportare rischi per la sicurezza. Contattare il rivenditore locale per la disponibilità degli accessori autorizzati.
- L'uso di questo prodotto in modo non consigliato nelle istruzioni fornite potrebbe comportare il rischio di incendio o lesioni personali.

# SERVIZIO E SUPPORTO

Visita il nostro sito multi-lingua a https://www.asus.com/support/.