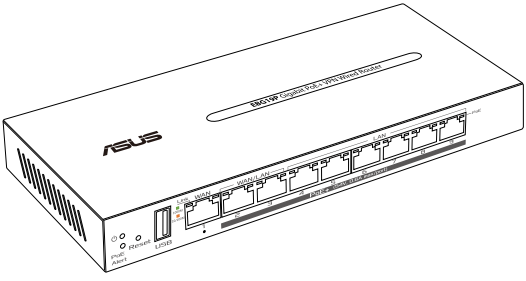
Manuale utente

ASUS EBG19P

Router cablato VPN Gigabit PoE+

Modello: EBG19P



IN SEARCH OF INCREDIBLE

I27419
Seconda Edizione
Marzo 2026

INFORMAZIONI SUL COPYRIGHT

Nessuna parte di questo manuale, compresi i prodotti e i software in esso descritti, può essere riprodotta, trasmessa, trascritta, archiviata in un sistema di recupero o tradotta in alcuna lingua, in alcuna forma e in alcun modo, fatta eccezione per la documentazione conservata dall'acquirente a scopi di backup, senza l'espressa autorizzazione scritta di ASUSTeK COMPUTER INC. ("ASUS").
ASUS FORNISCE QUESTO MANUALE "COSÌ COM'È" SENZA GARANZIA DI ALCUN TIPO, ESPLICITA O IMPLICITA, INCLUDENDO SENZA LIMITAZIONI LE GARANZIE O CONDIZIONI IMPLICITE DI COMMERCIABILITÀ O IDONEITÀ AD UN PARTICOLARE SCOPO. IN NESSUN CASO ASUS, I SUOI DIRIGENTI, FUNZIONARI, IMPIEGATI O DISTRIBUTORI SONO RESPONSABILI PER QUALSIASI DANNO INDIRETTO, PARTICOLARE, ACCIDENTALE O CONSEGUENTE (COMPRESI DANNI DERIVANTI DA PERDITA DI PROFITTO, PERDITA DI CONTRATTI, PERDITA D'USO O DI DATI, INTERRUZIONE DELL'ATTIVITÀ E SIMILI), ANCHE SE ASUS È STATA AVVISATA DELLA POSSIBILITÀ CHE TALI DANNI SI POSSANO VERIFICARE IN SEGUITO A QUALSIASI DIFETTO O ERRORE NEL PRESENTE MANUALE O NEL PRODOTTO.
I prodotti e nomi delle aziende che compaiono in questo manuale possono essere marchi registrati o diritti d'autore delle rispettive aziende, o meno, e sono usati a solo scopo identificativo o illustrativo, a beneficio dell'utente, senza alcuna intenzione di violazione dei diritti di alcun soggetto.
LE SPECIFICHE E LE INFORMAZIONI CONTENUTE IN QUESTO MANUALE SONO FORNITE A SOLO USO INFORMATIVO E SONO SOGGETTE A CAMBIAMENTI IN QUALSIASI MOMENTO, SENZA PREAVVISO, E NON POSSONO ESSERE INTERPRETATE COME UN IMPEGNO DA PARTE DI ASUS. ASUS NON SI ASSUME ALCUNA RESPONSABILITÀ E NON SI FA CARICO DI ALCUN ERRORE O INESATTEZZA CHE POSSA COMPARIRE IN QUESTO MANUALE COMPRESI I PRODOTTI E I SOFTWARE DESCRITTI AL SUO INTERNO.
Copyright © 2026 ASUSTeK Computer, Inc. Tutti i diritti riservati.

CONDIZIONI E LIMITI DI COPERTURA DELLA GARANZIA SUL PRODOTTO

Le condizioni di garanzia variano a seconda del tipo di prodotto e sono specificatamente indicate nel Certificato di Garanzia allegato a cui si fa espresso rinvio.
Inoltre la garanzia stessa non è valida in caso di danni o difetti dovuti ai seguenti fattori: (a) uso non idoneo, funzionamento o manutenzione impropri inclusi (senza limitazioni) e l'utilizzo del prodotto con una finalità diversa da quella conforme alle istruzioni fornite da ASUSTeK COMPUTER INC. in merito all'idoneità di utilizzo e alla manutenzione; (b) installazione o utilizzo del prodotto in modo non conforme agli standard tecnici o di sicurezza vigenti nell'Area Economica Europea e in Svizzera; (c) collegamento a rete di alimentazione con tensione non corretta; (d) utilizzo del prodotto con accessori di terzi, prodotti o dispositivi ausiliari o periferiche; (e) tentativo di riparazione effettuato da una qualunque terza parte diversa dai centri di assistenza ASUSTeK COMPUTER INC. autorizzati; (f) incidenti, fulmini, acqua, incendio o qualsiasi altra causa il cui controllo non dipenda da ASUSTeK COMPUTER INC.; (g) abuso, negligenza o uso commerciale. La Garanzia non è valida per l'assistenza tecnica o il supporto per l'utilizzo del Prodotto in merito all'utilizzo dell'hardware o del software. L'assistenza e il supporto disponibili (se previsti) 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**

DICHIARAZIONE DI ACCESSIBILITÀ

ASUS si impegna a rendere la nostra documentazione accessibile, in conformità alla Direttiva (UE) 2019/882 del Parlamento Europeo e del Consiglio. Questo documento è progettato per soddisfare i requisiti di WCAG 2.1 (livello AA)/EN 301 549 ed essere accessibile ai lettori di schermo come NVDA Screen Reader o Microsoft Narrator.

Per ulteriori informazioni sul prodotto, fare riferimento alla pagina web del prodotto:

https://qr.asus.com/networking/asus-expertwifi-ebg19p

Servizio e supporto

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

Indice

1 Presentazione dell'EBG19P

1.1 Benvenuti! 9
1.2 Contenuto della confezione 9
1.3 Il vostro router cablato 10
1.4 Posizionamento del router 12
1.5 Requisiti per l'installazione 13

2 Per iniziare

2.1 Configurazione del router 14
FAQ (Domande e risposte frequenti) 14
Connessione cablata 15
2.2 Accedere all'interfaccia web 16
2.3 Rilevamento automatico della WAN 17
FAQ (Domande e risposte frequenti) 17

3 Tutorial

ExpertWiFi 19

4 Configurare le EBG19P

4.1 Adattatore Adaptive QoS 20
4.1.1 Monitoraggio larghezza di banda 20
4.1.2 QoS 21
4.1.3 Cronologia web 21
4.1.4 Velocità Internet 22
4.2 Amministrazione 23
4.2.1 Modalità operativa 23
4.2.2 Sistema 24
4.2.3 Aggiornamento firmware 25
4.2.4 Ripristina/Salva/Carica Impostazioni 26

4.2.5 Feedback 27
4.2.6 Privacy 28
4.3 AiMesh 29
4.3.1 Configurazione del sistema ExpertWiFi AiMesh ... 29
4.3.2 Gestione dei client di rete 30
4.4 AiProtection 31
4.4.1 Protezione della rete 31
4.5 Dashboard 34
4.6 Controllo di accesso al dispositivo 35
4.6.1 Filtro web e app 35
4.6.2 Pianificazione temporale 36
4.7 Firewall 37
4.7.1 Generale 37
4.7.2 Filtro URL 38
4.7.3 Filtro parole chiave 39
4.7.4 Packet Filter 40
4.8 IPv6 41
4.9 LAN 42
4.9.1 LAN IP 42
4.9.2 Server DHCP 43
4.9.3 Rotte 45
4.9.4 IPTV 46
4.9.5 Controllo dello switch 46
4.9.6 VLAN 47
4.10 Strumenti di rete 49
4.10.1 Analisi di rete 49
4.10.2 Netstat 49
4.10.3 Riattivazione LAN 49
4.10.4 Regola di Connessione smart 49
4.11 SDN 50
4.11.1 Dipendente 51

4.11.2 Portale guest 51
4.11.3 Rete ospiti 52
4.11.4 Rete programmata 52
4.11.5 Rete IoT 53
4.11.6 Rete VPN 53
4.11.7 Esploratore di scenari 54
4.11.8 Rete personalizzata 55
4.12 Registro di sistema 56
4.13 Analizzatore del traffico 57
4.13.1 Analizzatore del traffico 57
4.14 Applicazioni USB 58
4.14.1 Server multimediale 58
4.14.2 Condivisione Risorse di rete (Samba 59
4.14.3 Condivisione FTP 59
4.14.4 Server stampante di rete 60
4.14.5 Modem USB 68
4.15 Fusione VPN 69
4.15.1 Creazione di una fusione VPN 69
4.15.2 Connessione ad Internet 70
4.16 Server VPN 71
4.16.1 PPTP 71
4.16.2 OpenVPN 72
4.16.3 IPSec VPN 73
4.16.4 VPN WireGuard® 74
4.17 WAN 75
4.17.1 Connessione ad Internet 75
4.17.2 Multi-WAN 77
4.17.3 Port Trigger 79
4.17.4 Virtual Server/Port Forwarding 81
4.17.5 DMZ 84
4.17.6 DDNS 85
4.17.7 NAT Passthrough 86

4.18 Wireless 87
4.18.1 Generale 87
4.18.2 Filtro MAC Wireless 88
4.18.3 Elenco dei blocchi di roaming 89

5 Risoluzione dei problemi

5.1 Risoluzione dei problemi più comuni 90
5.2 Domande e risposte frequenti (FAQs) 92

Appendice

Comunicazioni sulla sicurezza 110
Avviso WEEE 112

1 Presentazione dell'EBG19P

1.1 Benvenuti!

Vi ringraziamo per aver acquistato il router senza fili ASUS EBG19P!

EBG19P fornisce una rete veloce, sicura e scalabile, stabilità di rete migliorata tramite connettività Ethernet e fornisce backup Internet con due porte WAN/LAN e una porta USB per supportare le operazioni.

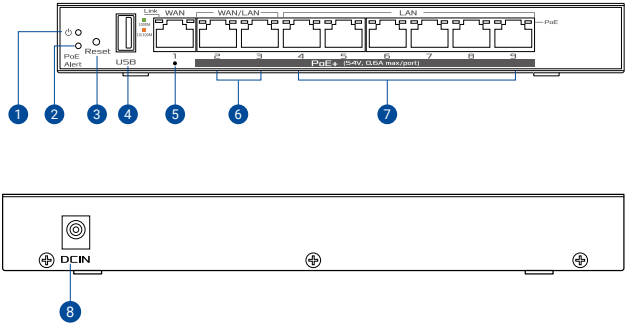
1.2 Contenuto della confezione

- EBG19P
- Cavo di rete Ethernet (RJ-45)
- Adattatore di alimentazione
- Guida rapida
- Adesivo con informazioni di accesso locale
- Certificato di garanzia

NOTE:

- Nel caso in cui uno di questi articoli sia danneggiato, o mancante, contattate ASUS per ottenere supporto. Fate riferimento a *Servizio e Supporto* in questo manuale utente.
- 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 cablato



1. LED alimentazione

Spento: Nessuna alimentazione.

Acceso: Il dispositivo è pronto.

Lampeggiante lentamente: Modalità di recupero.

2. LED di aviso PoE

Spento: Nessuna alimentazione o nessuna connessione fisica.

Acceso: L'alimentazione viene fornita a un dispositivo collegato alla porta PoE+.

NOTA: Puoi controllare lo stato di funzionamento del router nell'app ExpertWiFi.

3. Pulsante di reset

Questo pulsante serve a ripristinare le impostazioni predefinite di fabbrica.

4. Porta USB 3.2 Gen 1

Inserire un dispositivo compatibile con USB 3.2 Gen 1, come un disco rigido USB o una chiavetta USB, in questa porta.

5. Porta Internet (WAN)

Collegate un cavo di rete in questa porta per stabilire una connessione WAN. La porta è identificata da un punto tattile.

6. Porte WAN/LAN (con PoE+)

Collegate i cavi di rete in queste porte per stabilire connessioni WAN/LAN.

7. Porte LAN (con PoE+)

Collegate i cavi di rete in queste porte per stabilire connessioni LAN.

8. Porta ingresso alimentazione (DCIN)

Inserite l'alimentatore in dotazione in questo ingresso e collegate il router ad una sorgente di alimentazione.

Indicazioni LED della porta Ethernet

Indicatori LED			
LED Velocità (Verde)		**LED Link/Act LED (Giallo)**	
1Gbps	ACCESO	1Gbps/100Mbps/10Mbps	Lampeggiante
100Mbps/10Mbps	SPENTO	Nessun traffico	ACCESO

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): +54V con corrente massima 2,778A

  Temperatura di esercizio: 0 a 40°C

  Temperatura di stoccaggio: 0 a 70°C

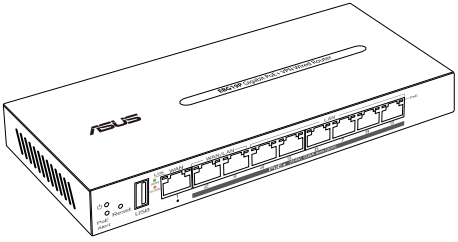
  Umidità di esercizio: 50 a 90%

  Umidità di stoccaggio: 20 a 90%

1.4 Posizionamento del router

Per la migliore esperienza di rete, assicurarsi di quanto segue:

- Aggiornate sempre all'ultimo firmware disponibile. Scaricate l'ultimo firmware disponibile dal sito web ASUS: https://www.asus.com.



1.5 Requisiti per l'installazione

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

- Porta (LAN) Ethernet RJ-45 (10Base-T/100Base-TX/1000BaseTX)
- Protocollo TCP/IP installato sul sistema operativo
- Un browser Internet come Internet Explorer, Mozilla Firefox, Safari o Google Chrome

NOTA: Il cavo Ethernet RJ-45, usato per la connessione cablata, non deve essere lungo più di 100m.

2 Per iniziare

2.1 Configurazione del router

IMPORTANTE!

Prima di configurare il vostro router cablato 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 montare questa apparecchiatura a un'altezza superiore a 2 metri.
- Usa questo prodotto in ambienti la cui temperatura sia compresa tra 0℃ (32˚F) e 40℃ (104˚F).

FAQ (Domande e risposte frequenti)

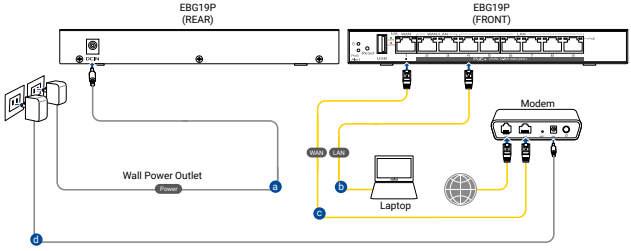
- Configurazione tramite l'app ExpertWiFi
- Impostazione tramite GUI Web (ASUSWRT)
- Impostazione tramite QIS (Installazione rapida Internet)

Connessione cablata

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

Per configurare il vostro router cablato 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. Aprire un browser web e accedere a http://expertwifi.net per la configurazione.

   Una volta eseguita la connessione l'interfaccia Web (GUI) si avvia automaticamente quando aprite un browser web. In caso contrario inserite http://expertwifi.net nella barra degli indirizzi.

3. Seguire le istruzioni per la configurazione.

2.2 Accedere all'interfaccia web

Il vostro router cablato ASUS dispone di un'interfaccia Web intuitiva, chiamata anche GUI (Graphical User Interface), che vi permette di configurare tutte le varie impostazioni disponibili tramite l'utilizzo di un browser Internet come, ad esempio, Microsoft Edge, Safari o Google Chrome.

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

Connessione cablata alla rete

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

1. Digitate http://expertwifi.net. nella barra degli indirizzi del vostro browser web.
2. Seguire le istruzioni per la configurazione.

2.3 Rilevamento automatico della WAN

FAQ (Domande e risposte frequenti)

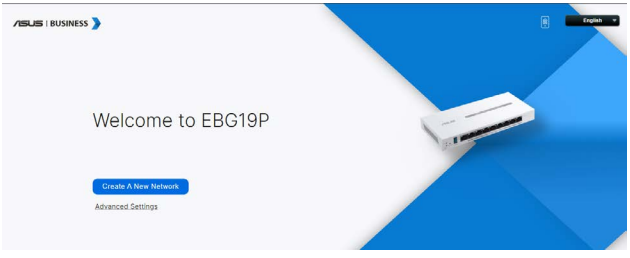
- Configurazione tramite l'app ExpertWiFi
- Impostazione tramite GUI Web (ASUSWRT)
- Impostazione tramite QIS (Installazione rapida Internet)

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

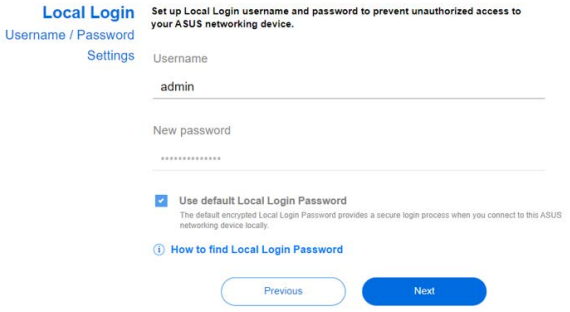
NOTA: Prima di impostare la connessione ad Internet per la prima volta assicuratevi di aver premuto il pulsante di Reset per riportare il router cablato alle impostazioni predefinite di fabbrica.

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

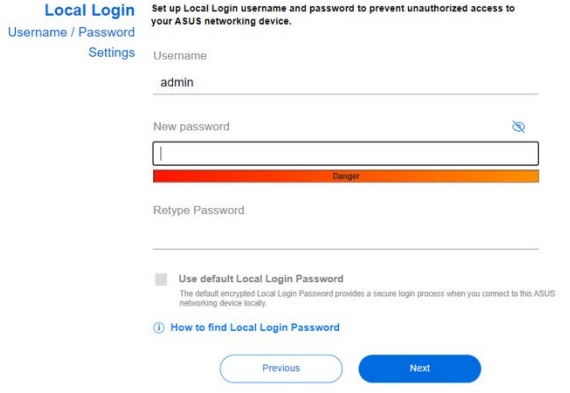
1. Entrate nell'interfaccia web e fare clic su **Create A New Network (Crea una nuova rete)**.



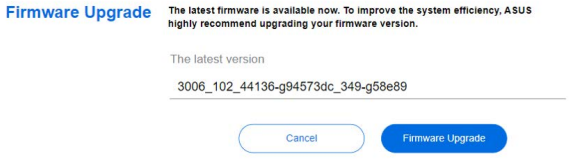
2. Fare clic su **Next (Avanti)** per accedere con il nome utente e la password predefiniti.



Deselezionare **Use default Local Login Password (Usa password di accesso locale predefinita)** e immettere un nuovo nome utente e una nuova password, quindi fare clic su **Next (Avanti)**.



3. Fare clic su Firmware Upgrade (Aggiornamento firmware) per aggiornare il firmware alla versione più recente oppure fare clic su Cancel (Annulla) per mantenere la versione attuale.



NOTA: La schermata viene visualizzata solo quando è disponibile una nuova versione del firmware.

3 Tutorial

ExpertWiFi

Configurazione Semplice della Scansione del Codice QR (Router ASUS serie ExpertWiFi)

Come accedo alla pagina di configurazione del mio router ExpertWiFi tramite Web GUI?

Cos'è una rete SDN (Self-Defined Network) e come configurare una SDN?

Come configurare lo switch ExpertWiFi in modalità ExpertWiFi AiMesh e modalità standalone?

Come affrontare i problemi di alimentazione instabile con un router cablato VPN gigabit PoE+ come ExpertWiFi EBG19P?

Come collegare un access point PoE a un router, switch o gateway?

Come regolare il canale WiFi e la larghezza di banda su diversi nodi ExpertWiFi AiMesh?

Come aggiungere uno switch PoE e un access point PoE come nodi AiMesh al mio router VPN cablato?

Come gestire i punti di accesso PoE tramite l'interfaccia Web GUI di ExpertWiFi?

Come configurare un gruppo multi-WAN su un router VPN ExpertWiFi?

Come configurare i dispositivi ExpertWiFi come nodi AiMesh?

Come aggiungere un sito ad ASUS Multi-Site Manager?

Come creare un gruppo in ASUS Multi-Site Manager?

Come impostare un Portale guest in una rete autodefinita (SDN) per fornire accesso a Internet ai dispositivi WiFi?

Come configurare le VLAN su un router ASUS ExpertWiFi?

Come rimuovere un dispositivo offline?

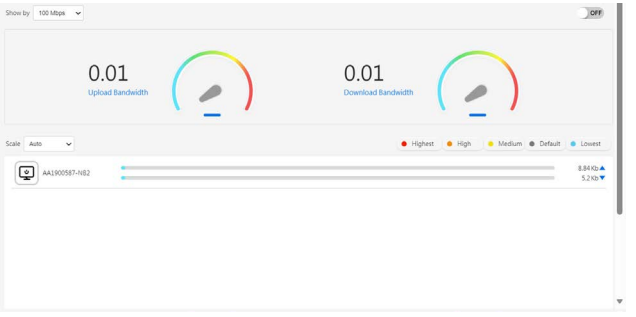
4 Configurare le EBG19P

4.1 Adattatore Adaptive QoS

4.1.1 Monitoraggio larghezza di banda

Il monitoraggio della larghezza di banda consente di monitorare l'utilizzo della larghezza di banda totale e di download e upload di ciascun client.

Per utilizzare **Bandwidth Monitor (Monitoraggio larghezza di banda)**, andare su **Settings (Impostazioni)** > **Adaptive QoS (QoS adattivo)** > **Bandwidth Monitor (Monitoraggio larghezza di banda)**.

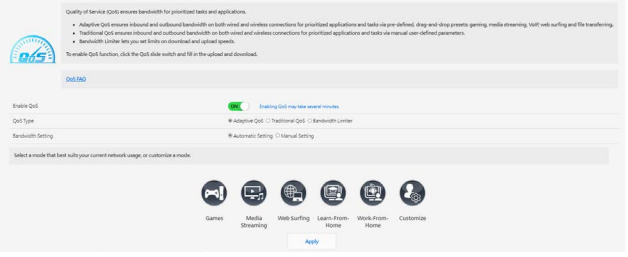


NOTA: Per altre informazioni, visitare https://www.asus.com/support/faq/1008717.

4.1.2 QoS

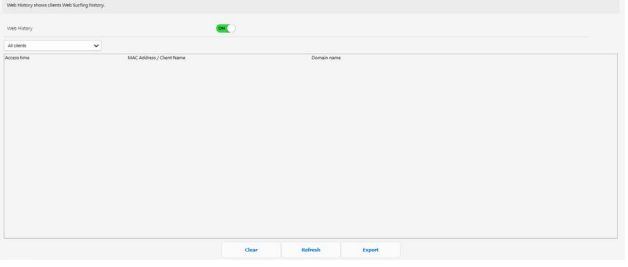
Qualità di servizio (QoS) garantisce la larghezza di banda per attività e applicazioni prioritarie.

1. **QoS adattivo** garantisce la larghezza di banda in entrata e in uscita su connessioni cablate e wireless per applicazioni e attività prioritarie tramite preimpostazioni di trascinamento predefinite: giochi, streaming multimediale, VoIP, navigazione sul web e trasferimento di file.
2. **QoS tradizionale** garantisce la larghezza di banda in entrata e in uscita su connessioni cablate e wireless per applicazioni e attività prioritarie tramite parametri manuali definiti dall'utente.
3. **Limitatore larghezza di banda** consente di impostare limiti sulla velocità di download e upload.



4.1.3 Cronologia web

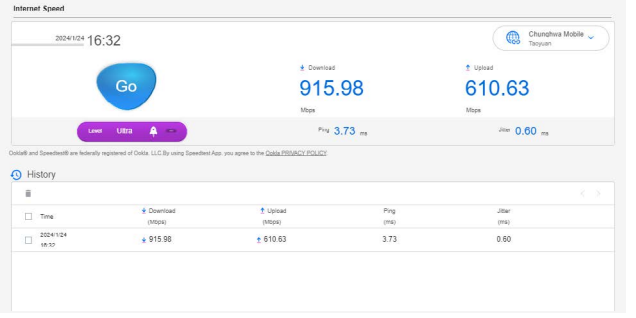
La pagina **Cronologia web** visualizza la cronologia di navigazione sul web dei client.



4.1.4 Velocità Internet

Questo servizio è fornito da Ookla®. Rileva la velocità di download e upload dal router a Internet.

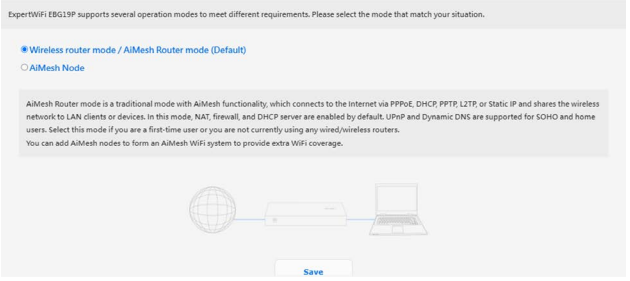
Fare clis su **VAI** per eseguire un test della velocità Internet, il cui completamento richiede circa un minuto.



4.2 Amministrazione

4.2.1 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 **Settings (Impostazioni)** > **Administration (Amministrazione)** > **Operation Mode (Modalità operativa)**.
2. Selezionate una delle seguenti modalità operative:
   - **Modalità router wireless / Modalità router AiMesh (Predefinita):** La modalità router AiMesh è una modalità tradizionale con funzionalità AiMesh, che si connette a Internet tramite PPPoE, DHCP, PPTP, L2TP o IP statico e condivide la rete wireless con i client o i dispositivi LAN. In questa modalità, NAT, Firewall e server DHCP sono abilitati per impostazione predefinita. UPnP e DNS dinamico sono supportati per utenti SOHO e domestici.
   - **Nodo AiMesh:** È possibile aggiungere nodi AiMesh per formare un sistema WiFi AiMesh al fine di fornire una copertura WiFi extra.
3. Quando avete finito cliccate su **Save (Salva)**.

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

4.2.2 Sistema

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

Per configurare le impostazioni di sistema:

1. Dal pannello di navigazione andate su **Settings (Impostazioni)** > **Administration (Amministrazione)** > **System (Sistema)**.
2. Potete configurare le seguenti impostazioni:
   - **Cambia le credenziali di accesso al router:** Potete cambiare la password e il nome utente del vostro router cablato inserendo un nuovo nome utente e una nuova password.
   - **Impostazioni USB:** In questa voce si può accedere alla funzione **Abilita ibernazione HDD** e cambiare la modalità USB.
   - **Time Zone (Fuso Orario):** Selezionate il corretto fuso orario per la vostra rete.
   - **Server NTP:** Il router cablato può ottenere informazioni da un server NTP (Network time Protocol) per regolare automaticamente data e ora.
   - **Monitoraggio di rete:** Potete abilitare Query DNS per controllare il nome host e l'indirizzo IP, o abilitare il Ping.
   - **Disconnessione automatica:** Per impostare il periodo di disconnessione automatica.
   - **Abilita reindirizzamento browser se WAN non disponibile:** Questa funzione permette al browser di visualizzare una pagina di avvertimento quando il router è disconnesso da Internet. Se disabilitata la pagina di avviso non apparirà.
   - **Abilita Telnet:** Selezionate **Yes (Sì)** per permettere le connessioni al router tramite il protocollo Telnet. Fare clic su **No** per disabilitare Telnet.
   - **Metodo d'autenticazione:** Potete scegliere HTTP, HTTPS o entrambi per un accesso al router sicuro.
   - **Abilita riavvio pianificato:** Quando abilitata potete impostare data e ora per il riavvio.
   - **Abilita l'accesso all'interfaccia Web da Internet:** Selezionate **Yes (Sì)** per permettere la gestione del router cablato tramite interfaccia Web anche dall'esterno della vostra rete. Selezionate **No** per impedirlo.

- **Abilita limitazioni di accesso:** Selezionate **Yes (Sì)** per creare un elenco di indirizzi IP ai quali permettere la gestione del router cablato tramite interfaccia Web da WAN/LAN.
- **Servizio:** Questa voce permette di configurare le funzioni Abilita Telnet/Abilita SSH/Porta SSH/ Allow Password Login/Authorized Keys/Timeout disconnessione.

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

4.2.3 Aggiornamento firmware

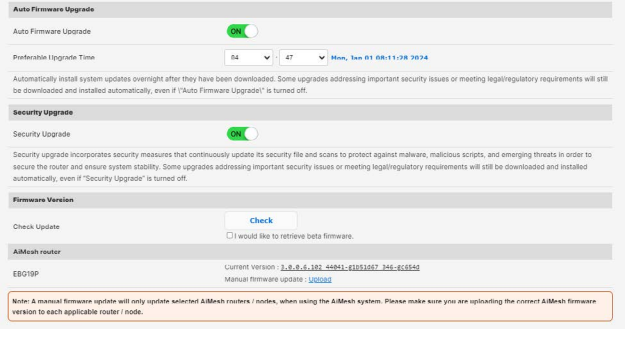
NOTA: Scaricate l'ultimo firmware disponibile dal sito web ASUS: https://www.asus.com.

Per aggiornare il firmware:

1. Dal pannello di navigazione andate su **Settings (Impostazioni)** > **Administration (Amministrazione)** > **Firmware Upgrade (Aggiornamento firmware)**.
2. Dalla pagina **New Firmware File (Nuovo file firmware)** cliccate su **Browse (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 cablato entra automaticamente in modalità di recupero e il LED di alimentazione del pannello anteriore comincia a lampeggiare lentamente.

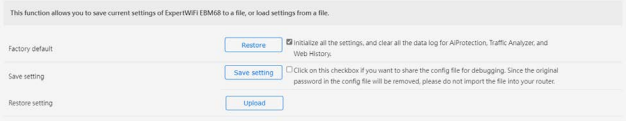


4.2.4 Ripristina/Salva/Carica Impostazioni

Per ripristinare/salvare/caricare le impostazioni del router cablato:

1. Dal pannello di navigazione andate su **Settings (Impostazioni)** > **Administration (Amministrazione)** > **Restore/Save/Upload Setting (Impostazione Ripristina/Salva/Carica)**.
2. Selezionate il processo che volete eseguire:
   - **Impostazioni predefinite:** Inizializzare tutte le impostazioni e cancellare tutto il registro dati per AiProtection, Analizzatore traffico e Cronologia web.
   - **Salva impostazioni:** Fare clic su questa casella di controllo se si desidera condividere il file di configurazione per il debug. Poiché la password originale nel file di configurazione viene rimossa, non importare il file nel router.
   - **Ripristina impostazioni:** Caricare le impostazioni di ripristino da applicare.

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



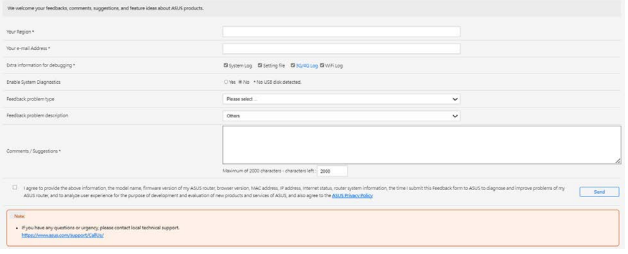
4.2.5 Feedback

Per utilizzare Feedback:

1. Dal pannello di navigazione, andare su **Settings (Impostazioni)** > **Administration (Amministrazione)** > **Feedback**.
2. Immettere regione, indirizzo e-mail, informazioni aggiuntive per il debug, commenti e suggerimenti e inviare il registro del router per la risoluzione dei problemi.

IMPORTANTE!

- Descrivere dettagliatamente i commenti sulla situazione per ottenere una risposta rapida.
- Accettare l'Informativa sulla privacy ASUS.



4.2.6 Privacy

1. **Per associazione account, DDNS e connessione remota (app ASUS Router/app Lyra/AiCloud/AiDisk):**

   Le informazioni dell'utente, inclusi il nome del modello del prodotto, la versione del firmware, lo stato di Internet, l'indirizzo IP, l'indirizzo MAC e il nome DDNS, vengono raccolti da ASUS attraverso le funzioni di cui sopra.

   Per disabilitare la condivisione delle informazioni con ASUS tramite le funzioni di cui sopra, fare clic su Withdraw (Ritira) di seguito. Tuttavia, queste caratteristiche/funzioni potrebbero non funzionare se si interrompe la condivisione delle informazioni con ASUS.

   IMPORTANTE!

   - Dopo aver fatto clic su Withdraw (Ritira), vengono apportate alcune modifiche elencate di seguito:
     - Il nome DDNS che si sta attualmente utilizzando non viene mantenuto nel router.
     - L'app Router ASUS, l'app Lyra, AiCloud, AiDisk possono essere utilizzati solo quando il dispositivo si trova nella stessa LAN del router.

2. **Informativa sulla privacy ASUS (per aggiornamento firmware/sicurezza):**

   Le informazioni vengono raccolte da Router ASUS per scopi di aggiornamento firmware/sicurezza. Per disabilitare la condivisione delle informazioni con ASUS, fare clic su **Withdraw (Ritira)** di seguito.

   IMPORTANTE! Facendo clic su **Withdraw (Ritira)** qui si potrebbe causare il mancato aggiornando al firmware più recente e la mancata protezione più aggiornata sul router ASUS. Tuttavia, per proteggere la sicurezza del router e garantire la conformità alle leggi, gli aggiornamenti che risolvono importanti problemi di sicurezza o soddisfano i requisiti legali/normativi vengono comunque scaricati e installati automaticamente.

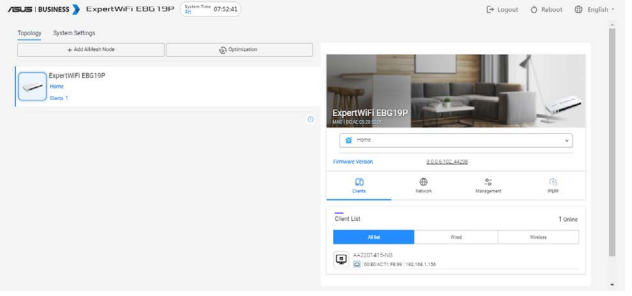
4.3 AiMesh

4.3.1 Configurazione del sistema ExpertWiFi AiMesh

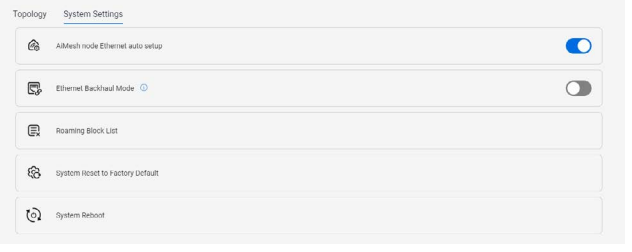
Per costruire il sistema ExpertWiFi AiMesh, è necessario configurarne le impostazioni.

Per configurare le impostazioni del sistema ExpertWiFi AiMesh:

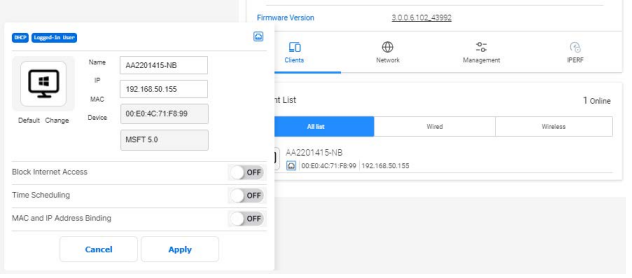
1. Dal pannello di navigazione, andare su **AiMesh** > **Topology (Topologia)**.
2. È possibile fare clic sulla parte inferiore di **Set up as AiMesh Node (Configura come nodo AiMesh)** per aggiungere i dispositivi ExpertWiFi sotto il controllo di EBG19P.



3. Andare su **AiMesh** > **System Settings (Impostazioni di sistema)** per abilitare o disabilitare **AiMesh node Ethernet auto setup (Configurazione automatica Ethernet del nodo AiMesh)**, **Ethernet Backhaul Mode (Modalità Ethernet Backhaul)**, configurare **Roaming Block List (Elenco dei blocchi di roaming)**, **System Reset to Factory Default (Ripristino del sistema alle impostazioni predefinite)** o **System Reset (Ripristino del sistema)**.



4.3.2 Gestione dei client di rete

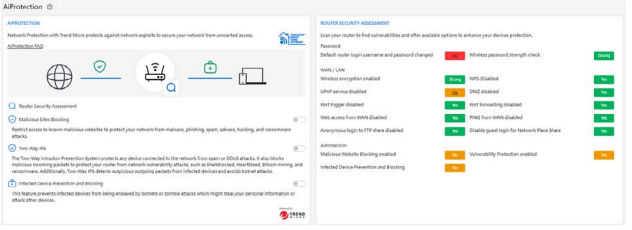


Per gestire i client della vostra rete:

1. Dal pannello di navigazione, andare su **AiMesh** > **Topology (Topologia)**.
2. Selezionare l'icona **Clients (Client)** per visualizzare le informazioni del client di rete come il nome del client, il MAC e l'indirizzo IP.
3. È possibile bloccare l'accesso del client alla rete, disabilitare la sua programmazione temporale o disabilitare l'associazione MAC e IP spostando il cursore su **OFF**.
4. Quando avete finito cliccate su **Apply (Applica)**.

4.4 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.

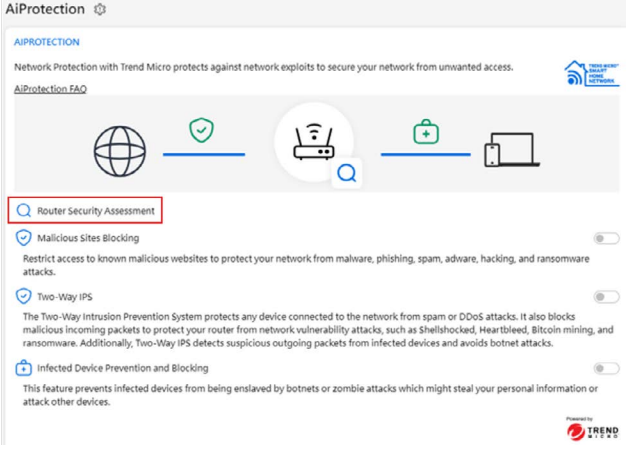


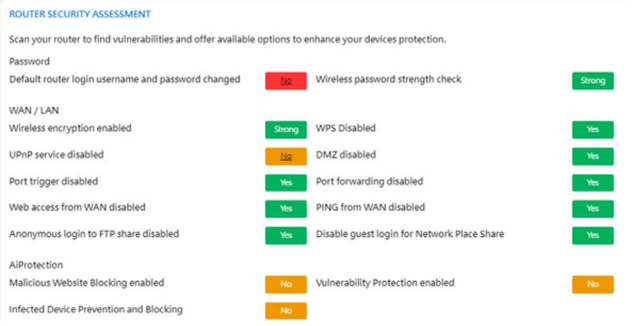
4.4.1 Protezione della rete

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

Per valutare la sicurezza del router:

1. Dal pannello di navigazione andate su **AiProtection**.
2. Fare clic su **Router Security Assessment (Valutazione della sicurezza del router)** per visualizzare i risultati della valutazione della sicurezza.





IMPORTANTE!Le voci sicure vengono valutate con un **Yes (Sì)** nella pagina **ROUTER SECURITY ASSESSMENT (Valutazione della sicurezza del router)**. Al contrario le voci valutate con **No** devono essere configurate ulteriormente.

3. (Opzionale) Nella pagina **ROUTER SECURITY ASSESSMENT (VALUTAZIONE DELLA SICUREZZA DEL ROUTER)** configurate manualmente le voci valutate con **No**. Per fare questo:
   a. Cliccate su una voce.

   NOTA: Quando cliccate su una voce verrete reindirizzati automaticamente alla pagina delle sue impostazioni.

   b. Configurate e applicate le modifiche necessarie, cliccate su **Apply (Applica)** quando avete finito.
   c. Tornate alla pagina **ROUTER SECURITY ASSESSMENT (VALUTAZIONE DELLA SICUREZZA DEL ROUTER)** e cliccate su **Close (Chiudi)** per uscire.
4. Per configurare automaticamente le opzioni di sicurezza cliccate su **Secure Your Router (Metti in sicurezza)**.
5. Quando appare un messaggio di conferma cliccate su OK.

Per abilitare la protezione della rete:

1. Dal pannello di navigazione andate su **AiProtection**.
2. Selezionare il tipo di protezione da implementare e scorrerla. È possibile scegliere tra **Malicious Sites Blocking (Blocco siti pericolosi), Two-Way IPS (IPS bidirezionale) e Infected Device Prevention and Blocking (Prevenzione e blocco di dispositivi infetti)**.

Blocco siti web malevoli

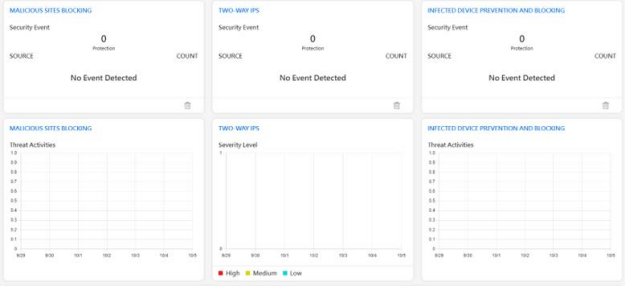
Questa funzionalità limita l'accesso a siti web pericolosi noti per proteggere la rete da attacchi malware, phishing, spam, adware, hacking e ransomware.

IPS bidirezionale

IPS bidirezionale (Intrusion Prevention System-Sistema di prevenzione delle intrusioni) protegge i dispositivi connessi da spam o attacchi DDoS. Blocca inoltre i pacchetti pericolosi in entrata per proteggere il router da attacchi di vulnerabilità della rete, come Shellshocked, Heartbleed, Bitcoin mining e ransomware. Inoltre, IPS bidirezionale rileva i pacchetti sospetti in uscita dai dispositivi infetti ed evita gli attacchi di botnet.

Prevenzione e blocco di dispositivi infetti

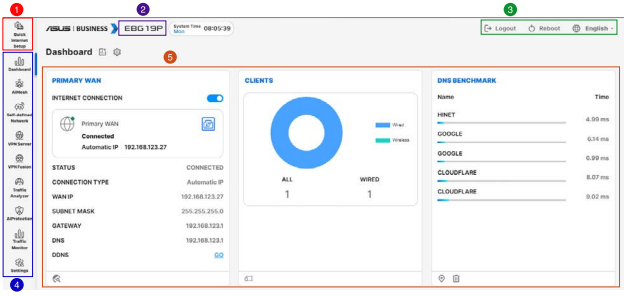
Questa funzionalità impedisce che i dispositivi infetti vengano controllati da botnet o attacchi zombie che potrebbero rubare i dati personali o attaccare altri dispositivi.



3. Accettare il **Trend Micro End User License Agreement (Contratto di licenza con l'utente finale Trend Micro)**.

4.5 Dashboard

Dashboard consente di gestire la rete come connessione Internet, connessione client, benchmark DNS, stato del sistema, porta Ethernet e monitoraggio del traffico.



1. QIS (Quick Internet Setup)
2. Nome modello
3. Pulsanti di comando
4. Pannello di navigazione
5. Informazioni del cruscotto

4.6 Controllo di accesso al dispositivo

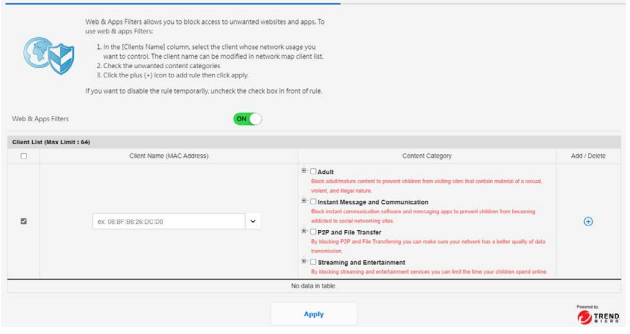
4.6.1 Filtro web e app

La funzione Filtri web e app consente di bloccare l'accesso a siti web e app indesiderati.

Per utilizzare Filtri web e app:

1. Dal pannello di navigazione andate su **Settings (Impostazioni)** > **Device access control (Controllo di accesso al dispositivo)** > **Web & Apps Filters (Filtro web e app)**.
2. Far scorrere la barra su **ON** per abilitare **Web & Apps Filters (Filtri web e app)**.
3. Nella colonna **Client Name (Nome client)**, selezionare il client di cui si desidera controllare l'utilizzo della rete. Il nome del client può essere modificato nell'elenco dei client della mappa di rete.
4. Controllare le categorie di contenuti indesiderati.
5. Fare clic su ⊕ per aggiungere una regola e fare clic su **Apply (Applica)**.

Per disattivare temporaneamente una regola, deselezionarla.

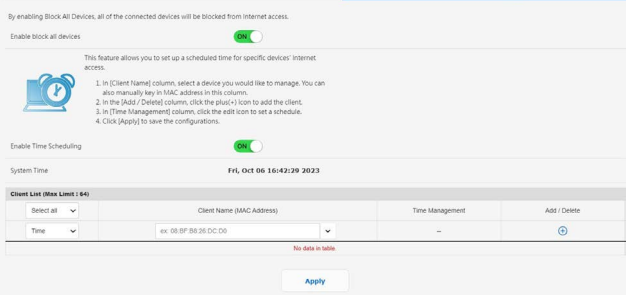


4.6.2 Pianificazione temporale

La programmazione temporale consente di impostare un orario programmato per l'accesso a Internet di dispositivi specifici.

Per utilizza Pianificazione temporale:

1. Dal pannello di navigazione andate su **Settings (Impostazioni)** > **Device access control (Controllo di accesso al dispositivo)** > **Time Scheduling (Pianificazione temporale)**.
2. Far scorrere la barra su **ON** per abilitare **Enable Time Scheduling (Abilita Pianificazione temporale)**.
3. Nella colonna **Client Name (Nome client)** selezionate o inserite il nome del client.
4. Cliccate su ⊕ per aggiungere il profilo del client.
5. Cliccate su **Apply (Applica)** per confermare le modifiche.



4.7 Firewall

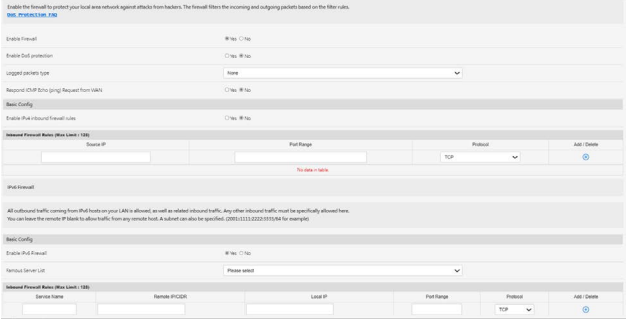
4.7.1 Generale

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

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

Per configurare le impostazioni di base del firewall:

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



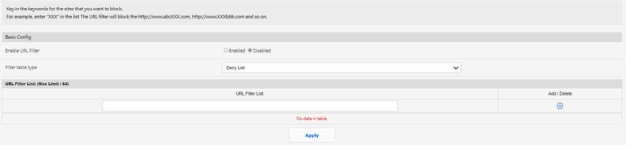
4.7.2 Filtro URL

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 **Settings (Impostazioni)** > **Firewall** > **URL filter (Filtro URL)**.
2. Alla voce **Enable URL Filter (Abilita filtro URL)** selezionate **Enabled (Abilitato)**.
3. Inserite un indirizzo Internet e cliccate su ⊕.
4. Cliccate su **Apply (Applica)**.



4.7.3 Filtro parole chiave

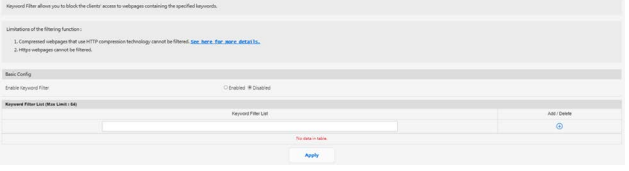
Il Filtro Parole Chiave blocca l'accesso alle pagine web contenenti le parole che inserite nell'elenco.

Per abilitare e configurare il Filtro Parole Chiave:

1. Dal pannello di navigazione andate su **Settings (Impostazioni)** > **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 su ⊕.
4. Cliccate su **Apply (Applica)**.

NOTE:

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

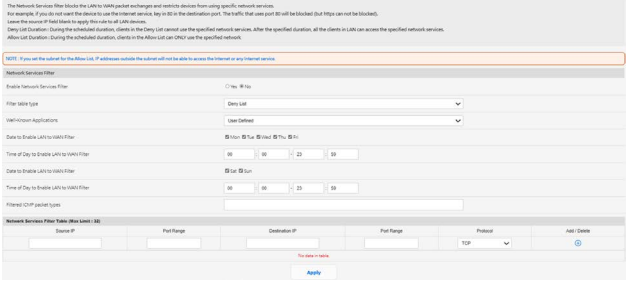


4.7.4 Packet Filter

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.

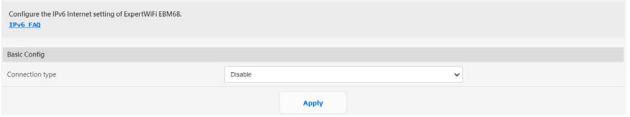
Per abilitare e configurare il Packet Filter:

1. Dal pannello di navigazione andate su **Settings (Impostazioni)** > **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. **Deny List (Elenco non consentiti)** blocca i servizi di rete selezionati. **Allow List (Elenco 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 su ⊕.
6. Cliccate su **Apply (Applica)**.



4.8 IPv6

Il router cablato supporta il protocollo IPv6, un protocollo in grado di gestire molti più indirizzi del protocollo IPv4. Chiedete informazioni al vostro ISP per sapere se IPv6 è effettivamente supportato.



Per configurare IPv6:

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

NOTE:

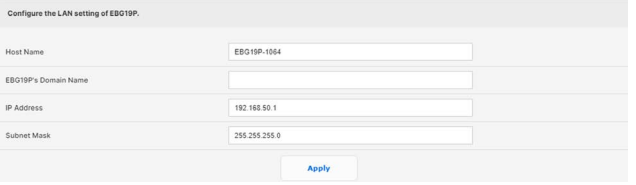
- Chiedete informazioni al vostro ISP per sapere se IPv6 è effettivamente supportato.
- Per altre informazioni, visitare https://www.asus.com/support/FAQ/113990.

4.9 LAN

4.9.1 LAN IP

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

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

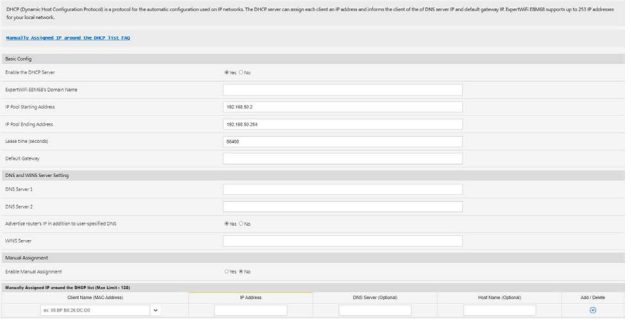


Per modificare le impostazioni LAN del router wireless:

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

4.9.2 Server DHCP

DHCP (Dynamic Host Configuration Protocol) è un protocollo per la configurazione automatica usato su reti IP. Il server DHCP può assegnare a ciascun client un indirizzo IP ed informare il client dell'IP del server DNS e dell'IP del gateway predefinito.



Per configurare il server DHCP:

1. Dal pannello di navigazione andate su **Settings (Impostazioni)** > **LAN** > **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 cablato.
4. Nel campo **IP Pool Starting Address (Indirizzo IP iniziale)** inserite l'indirizzo IP iniziale dell'intervallo desiderato.
5. Nel campo **IP Pool Ending Address (Indirizzo IP finale)** inserite l'indirizzo IP finale dell'intervallo desiderato.
6. Nel campo **Lease Time (Tempo di rilascio)** specificate, in termini di secondi, la durata dell'assegnazione di un indirizzo IP. Una volta raggiunto il tempo di rilascio il server DHCP assegnerà al client un nuovo indirizzo IP.

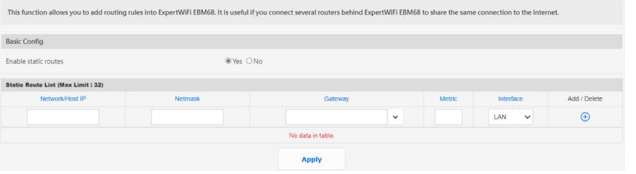
NOTE:

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

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

4.9.3 Rotte

Questa funzione consente di aggiungere regole di routing al router. È utile se si connettono diversi router dietro EBG19P per condividere la stessa connessione a Internet.

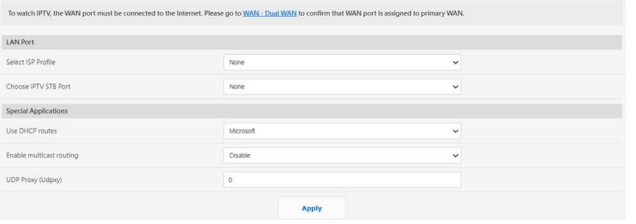


Per configurare la tabella di routing:

1. Dal pannello di navigazione andate su **Settings (Impostazioni)** > **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 ⊕ o ⊖ per aggiungere o rimuovere un dispositivo dall'elenco.
4. Cliccate su **Apply (Applica)**.

4.9.4 IPTV

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

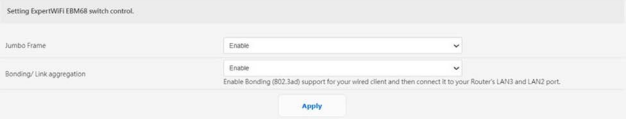


4.9.5 Controllo dello switch

Consente di configurare il router per la funzione di controllo dello switch. È possibile combinare due porte LAN da 1 Gbps per offrire velocità cablate fino a 2 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 la porta LAN3 alla porta LAN2.

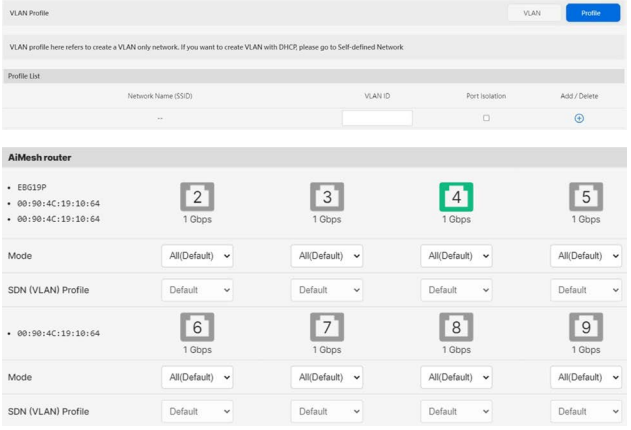


4.9.6 VLAN

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 **Settings (Impostazioni)** > **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 / 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/.

4.10 Strumenti di rete

Per utilizzare strumenti di rete, dal pannello di navigazione, andare su **Settings (Impostazioni)** > **Network Tools (Strumenti di rete)**.

4.10.1 Analisi di rete

Inviare pacchetti ICMP ECHO_REQUEST agli host di rete.

4.10.2 Netstat

Visualizza i dettagli della rete.

4.10.3 Riattivazione LAN

La funzione WOL (Wake-On-LAN) consente di attivare un computer da qualsiasi dispositivo della rete.

4.10.4 Regola di Connessione smart

Configura le informazioni relative alla Connessione smart.

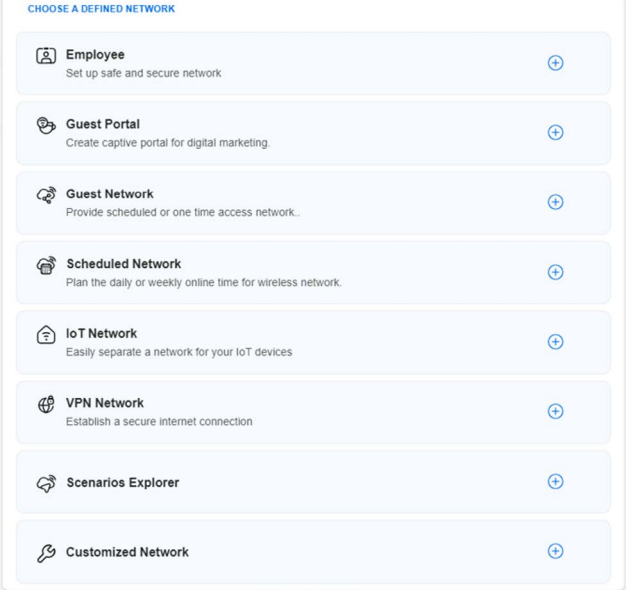
4.11 SDN

Una rete SDN (Self-Defined Network) fornisce fino a cinque SSID per separare e dare priorità ai dispositivi per diversi usi aziendali e alternative di rete, creando segmenti di rete per dipendenti, portali guest, reti guest, reti programmate, reti IoT e reti VPN.

IMPORTANTE! Per rendere disponibile la funzione Wi-Fi, assicurarsi di integrare un punto di accesso wireless (AP) come ExpertWiFi EBA63 o un router come ExpertWiFi EBR63 o ExpertWiFi EBM68 nella rete AiMesh dell'EBG19P.

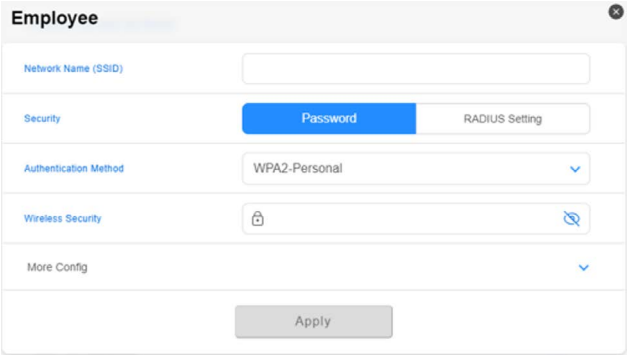
Per creare una SDN (Self-Defined Network):

1. Dal pannello di navigazione, andare su **SDN (Self-Defined Network)**.
2. Scegliere una rete definita adatta allo scenario specifico.



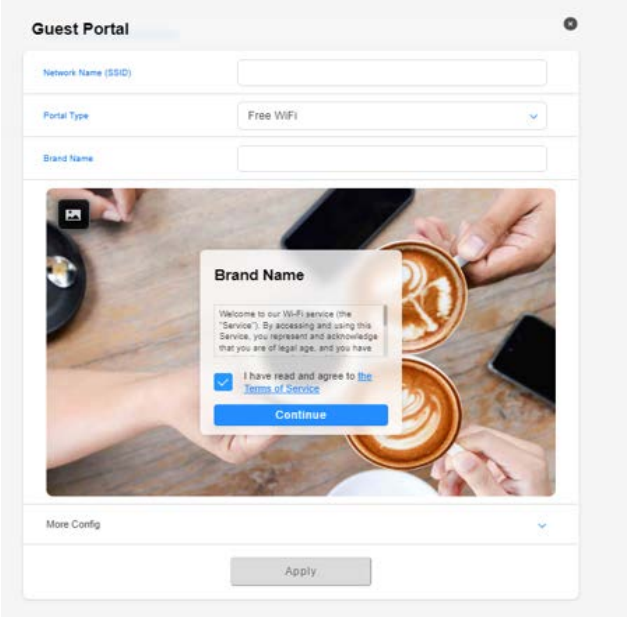
4.11.1 Dipendente

Consente di impostare il livello di accesso per diversi usi per migliorare la sicurezza della rete. Consigliato per uffici che assegnano autorizzazioni a diversi reparti.



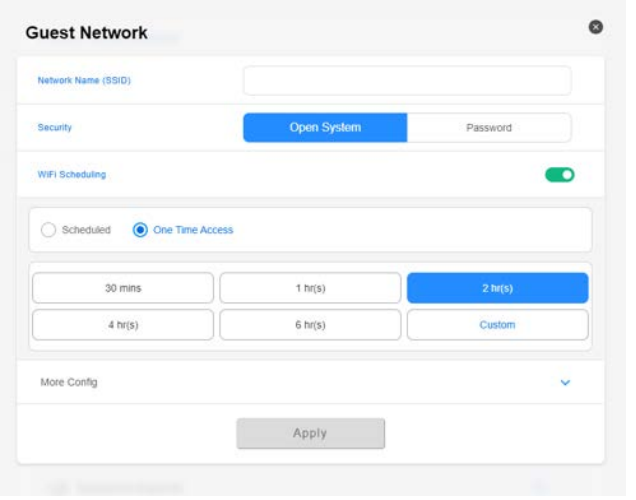
4.11.2 Portale guest

Consente di creare un portale guest per il marketing digitale. Consigliato per l'uso in ristoranti, hotel o food truck.



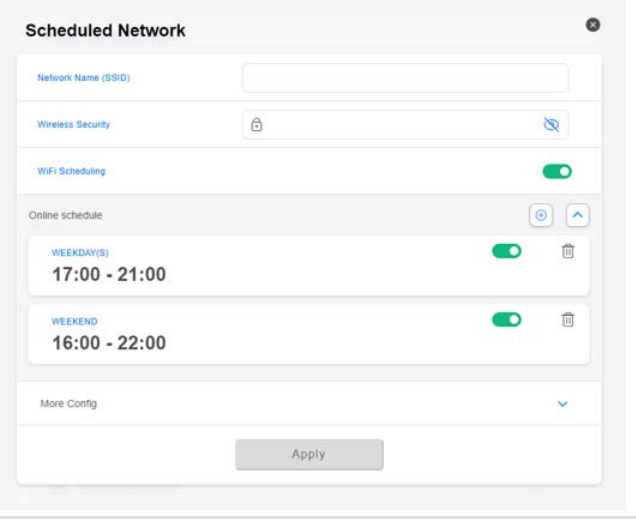
4.11.3 Rete ospiti

Fornisce ai visitatori temporanei un accesso programmato o una tantum alla rete. Consigliato per l'uso in centri commerciali, palestre o per visitatori.



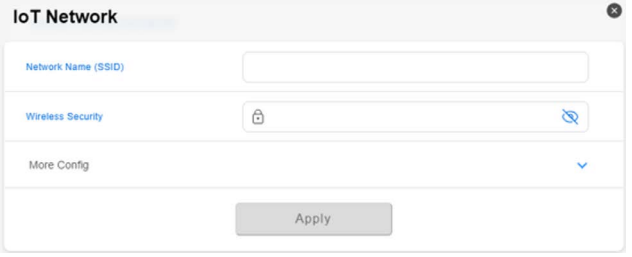
4.11.4 Rete programmata

Pianifica il tempo online giornaliero o settimanale per la rete wireless. Consigliato per l'apprendimento a distanza, in classe o per l'uso da parte dei bambini.



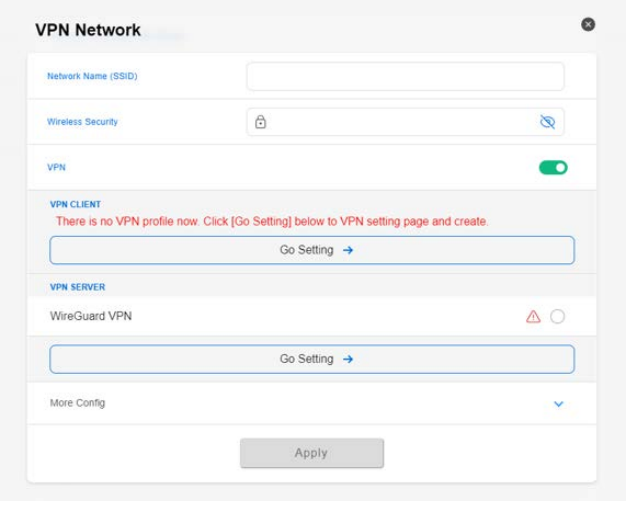
4.11.5 Rete IoT

Consente di configurare facilmente una rete separata per i dispositivi IoT. Consigliato per l'uso con dispositivi di sorveglianza, assistenti vocali, illuminazione, videocitofoni, serrature smart e sensori.



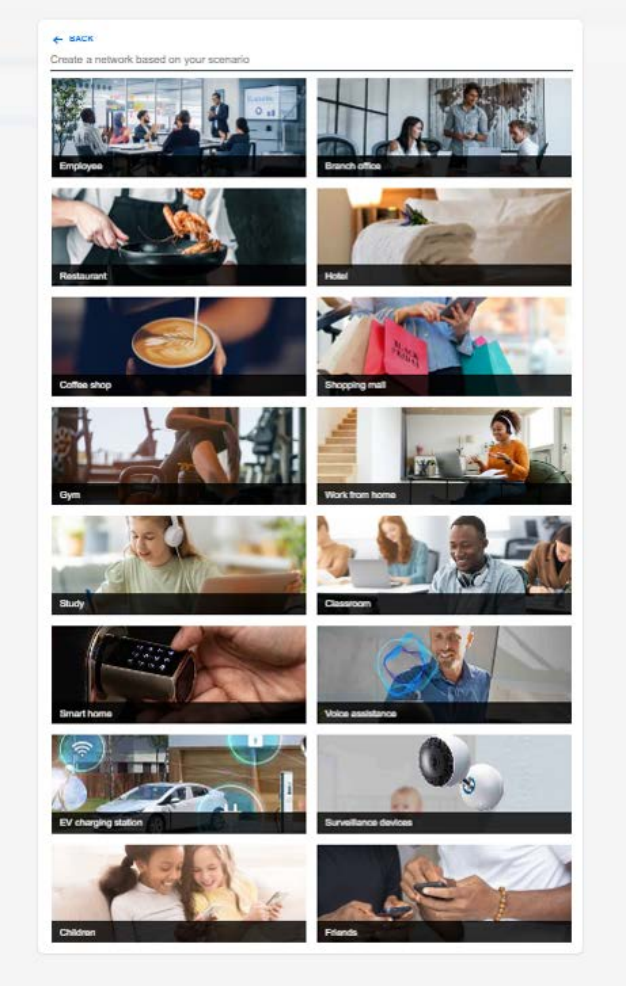
4.11.6 Rete VPN

Consente di stabilire una connessione Internet sicura tramite VPN.



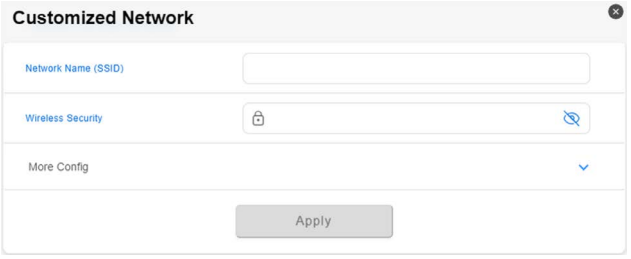
4.11.7 Esploratore di scenari

Se non si ha idea di quale rete creare, si può scegliere il settore che corrisponde alla propria affiliazione per creare la rete.



4.11.8 Rete personalizzata

Consente di selezionare l'opzione di una rete personalizzata.



4.12 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:

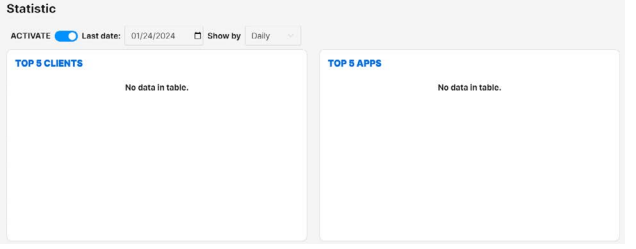
1. Dal pannello di navigazione andate su **Settings (Impostazioni)** > **System Log (Registro di sistema)**.
2. Potete visualizzare le diverse attività di rete in una delle seguenti schede:
   - Registro generale
   - Lease DHCP
   - Reindirizzamento delle porte
   - Tabella di routing
   - IPv6
   - Connessioni

4.13 Analizzatore del traffico

4.13.1 Analizzatore del traffico

Per utilizzare l'analizzatore di traffico:

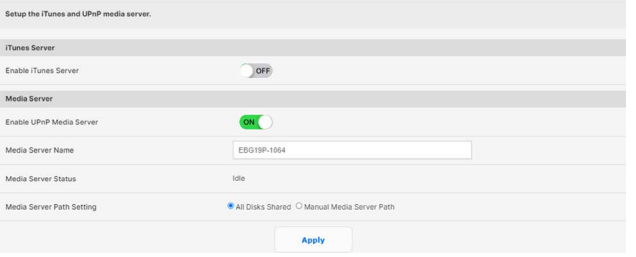
1. Attivare **ACTIVATE (ATTIVA)**.
2. Assegnare l'ultima data da mostrare e scegliere di monitorare il traffico di rete su base giornaliera, settimanale o mensile dall'elenco a discesa **Show by (Mostra per)**.
3. Vengono visualizzati i primi cinque client, le prime cinque app, i dispositivi, lo stato del client e l'analisi delle app.



4.14 Applicazioni USB

4.14.1 Server multimediale

Il server multimediale consente di configurare iTunes e il server UPnP.



Per lanciare le impostazioni del Server multimediale andate su **Settings (Impostazioni)** > **USB Application (Applicazioni USB)** > **Media Server (Server multimediale)**.

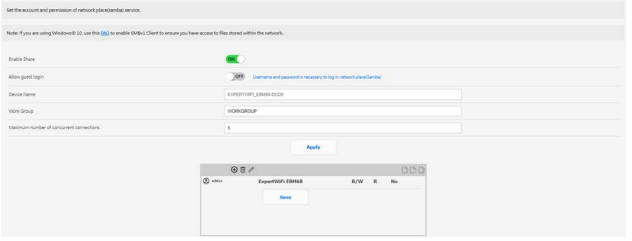
Fate riferimento alle seguenti informazioni in merito alle diverse voci presenti nel menu:

- **Abilitare il server iTunes:** Spostate il cursore su ON/OFF per abilitare/disabilitare il Server iTunes.
- **Abilita Server multimediale UPnP:** Spostate il cursore su ON/OFF per abilitare/disabilitare il Server multimediale UPnP.
- **Nome server multimediale:** Immette il nome del server multimediale.
- **Impostazioni percorso Server multimediale:** Selezionate All Disks Shared (Tutti i dischi condivisi) o Manual Media Server Path (Percorso manuale Server multimediale).

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

4.14.2 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, dal pannello di navigazione andate su **Settings (Impostazioni)** > **USB Application (Applicazioni USB)** > **Network Place (Samba) Share (Condivisione Risorse di rete (Samba))**.

4.14.3 Condivisione FTP

La condivisione FTP consente di configurare gli account e le autorizzazioni per il servizio FTP.

Per usare il servizio FTP Share (Condivisione FTP), dal pannello di navigazione andate su **Settings (Impostazioni)** > **USB Application (Applicazioni USB)** > **FTP Share (Condivisione FTP)**.

4.14.4 Server stampante di rete

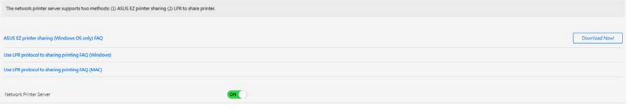
4.14.4.1 ASUS EZ Printer Sharing

ASUS EZ Printer Sharing vi permette di connettere una stampante USB alla porta USB del vostro router cablato 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 e Windows® 11.

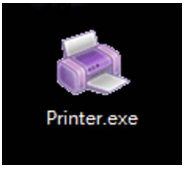
Per configurare la modalità condivisione stampante EZ:

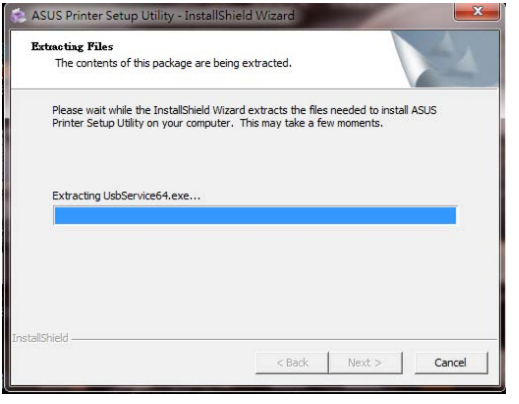
1. Dal pannello di navigazione andate su **Settings (Impostazioni)** > **USB Application (Applicazioni USB)** > **Network Printer Server (Server di stampa di rete)**.
2. Cliccate su **Download Now! (Scarica Adesso!)** per scaricare l'utility per la stampante di rete.



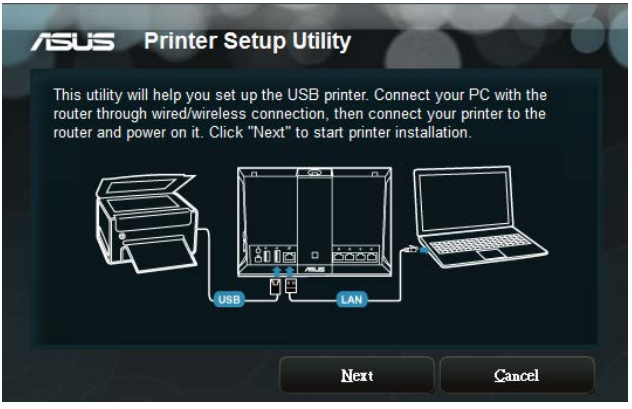
NOTA: L'utility per le stampanti di rete è supportata su Windows® 10 e Windows® 11. Per installare l'utility su Mac OS selezionate **Use LPR protocol for sharing printer (Usa il protocollo LPR per condividere la stampante)**.

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



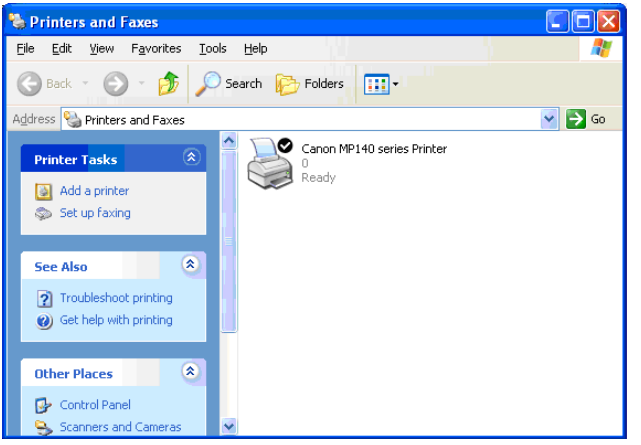


4. Seguite le istruzioni sullo schermo per completare il processo di installazione dell'hardware e poi cliccate su **Next (Avanti)**.



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® OS 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.

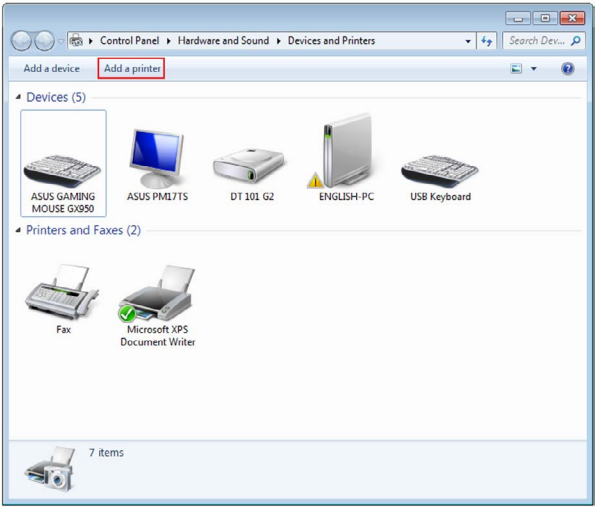


4.14.4.2 Utilizzo di LPR per condividere una stampante

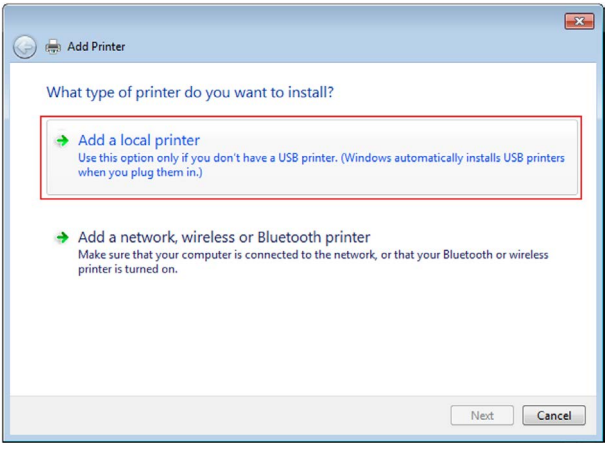
Potete condividere una stampante con i vostri computer Windows® e MAC usando il protocollo LPR/LPD (Line Printer Remote/Line Printer Daemon).

Per condividere la vostra stampante LPR:

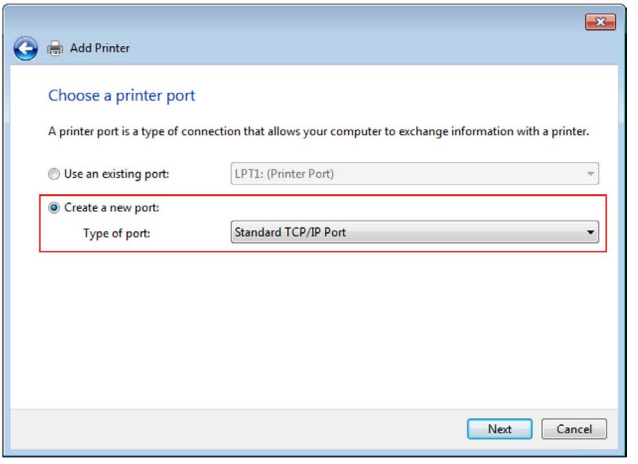
1. Dal Desktop di Windows® cliccate su **Start** > **Devices and Printers (Dispositivi e Stampanti)** > **Add a printer (Aggiungi stampante)** per far partire la procedura guidata **Add Printer Wizard (Aggiungi stampante)**.



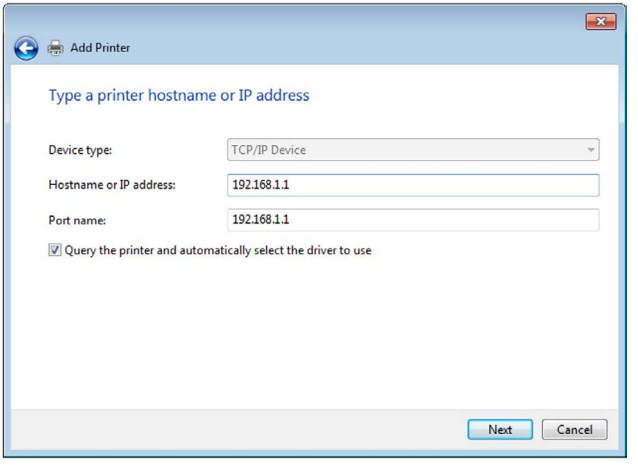
2. Selezionate **Add a local printer (Aggiungi stampante locale)** e poi cliccate su **Next (Avanti)**.



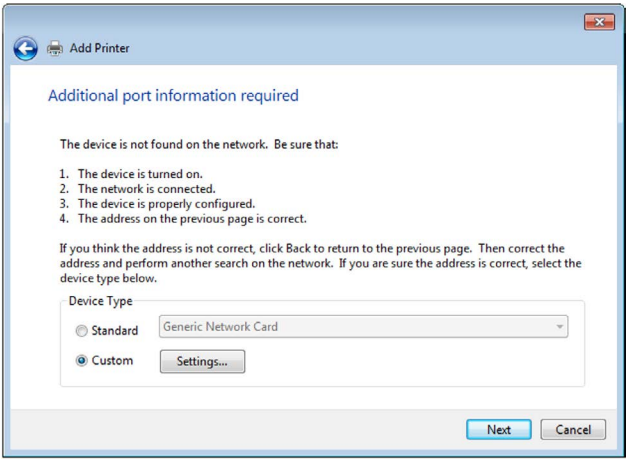
3. Selezionate **Create a new port (Crea una nuova porta)** e poi impostate **Type of Port (Tipo di porta)** su **Standard TCP/IP Port (Porta TCP/IP standard)**. Cliccate su **Next (Avanti)**.



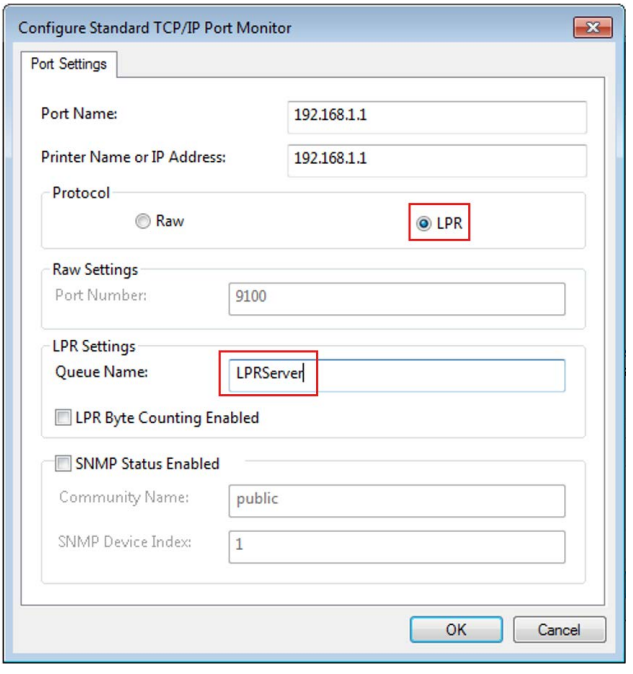
4. Nel campo **Hostname or IP address (Nome host o indirizzo IP)** inserite l'indirizzo IP del router cablato e poi cliccate su **Next (Avanti)**.



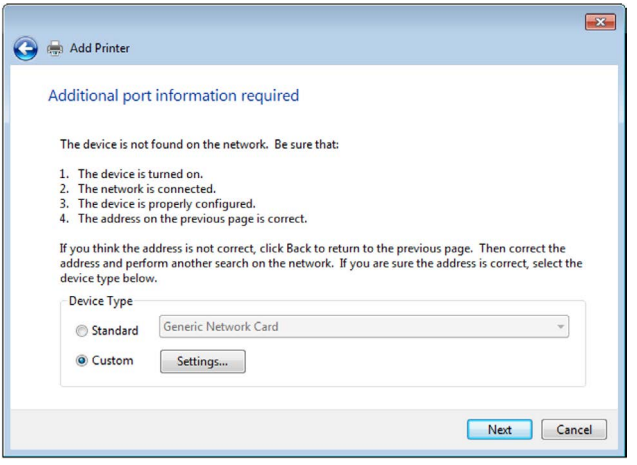
5. Selezionate **Custom (Personalizzata)** e poi cliccate su **Settings (Impostazioni)**.



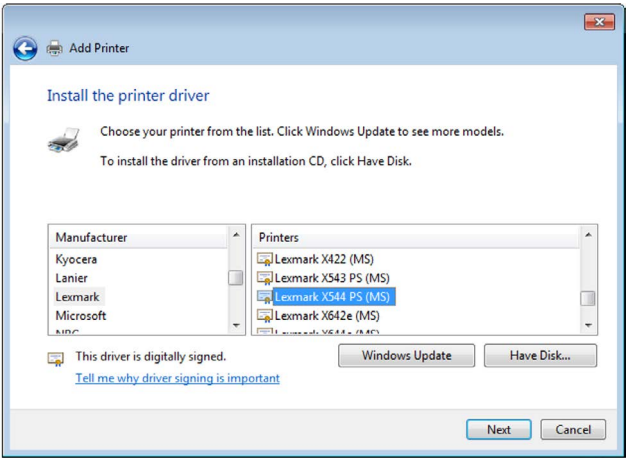
6. Impostate il **Protocol (Protocollo)** su **LPR**. Nel campo **Queue Name (Nome coda)** inserite **LPRServer** e poi cliccate su **OK** per continuare.



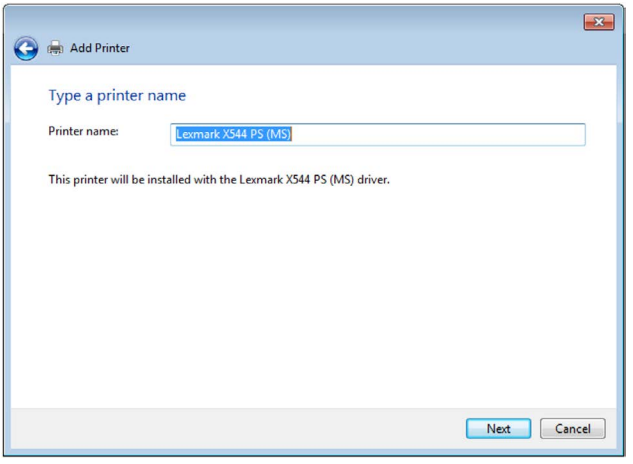
7. Cliccate su **Next (Avanti)** per completare le impostazioni della porta TCP/IP standard.



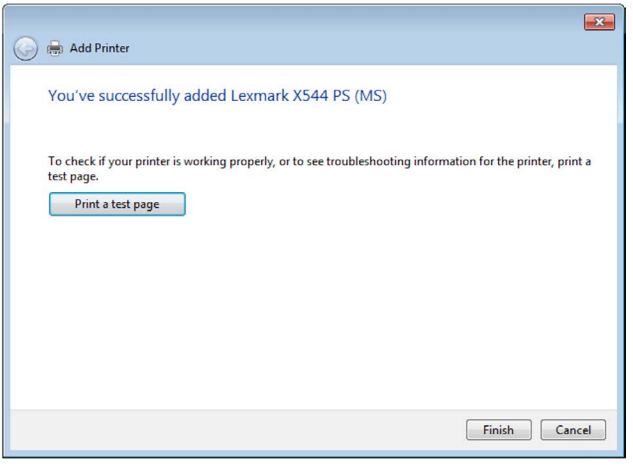
8. Installate i driver della stampante selezionando il produttore e il modello corretti dall'elenco. Se la vostra stampante non è nell'elenco cliccate su **Have Disk (Disco driver)** per installare i driver da un supporto CD-ROM o da un file manualmente.



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



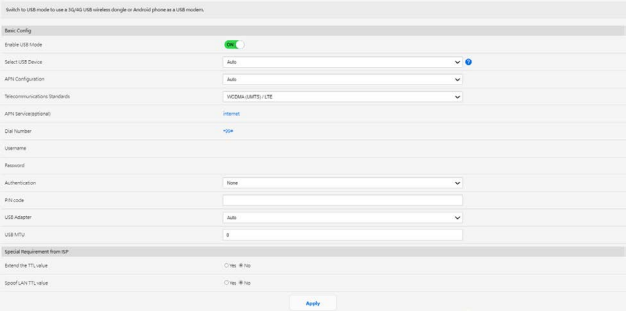
10. Cliccate su **Finish (Fine)** per completare l'installazione.



4.14.5 Modem USB

Consente di passare alla modalità USB per utilizzare un dongle wireless USB 3G/4G o un telefono Android come modem USB.

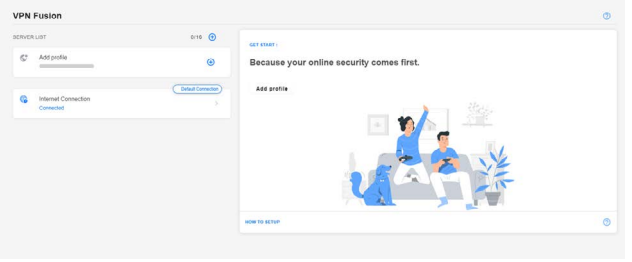
Per utilizzare il modem USB, andare su **Settings (Impostazioni)** > **USB Application (Applicazioni USB)** > **USB Modem (Modem USB)**.



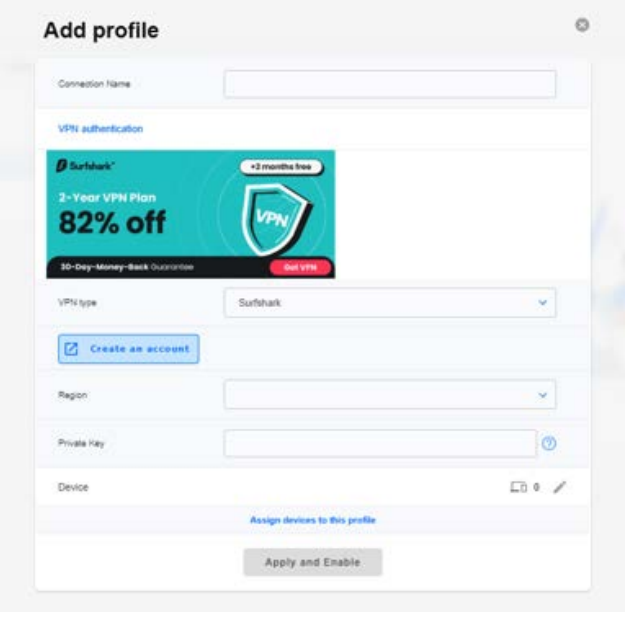
4.15 Fusione VPN

4.15.1 Creazione di una fusione VPN

VPN Fusion vi permette di connettervi a server VPN multipli in simultanea e assegna i vostri dispositivi client a tunnel VPN differenti.

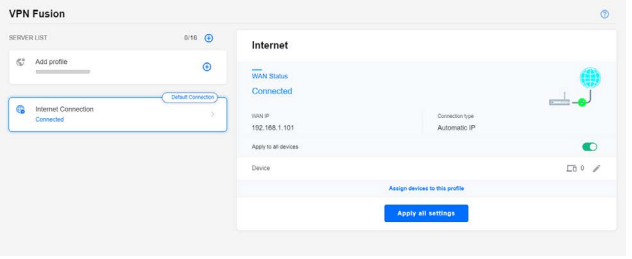


1. Dal pannello di navigazione, andare su **VPN Fusion (Fusione VPN)**.
2. Fare clic su ⊕ nel campo **Add profile (Aggiungi profilo)** per configutare un nuovo tunnel VPN.
3. Completare la configurazione della VPN includendo nome della connessione, tipo di VPN, regione, chiave privata e dispositivo.
4. Fare clic su **Apply and Enable (Applica e abilita)**.



4.15.2 Connessione ad Internet

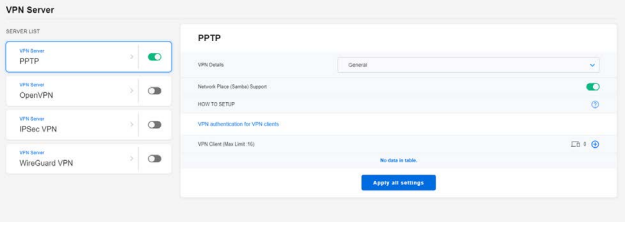
Consente di gestire lo stato WAN dei dispositivi connessi.



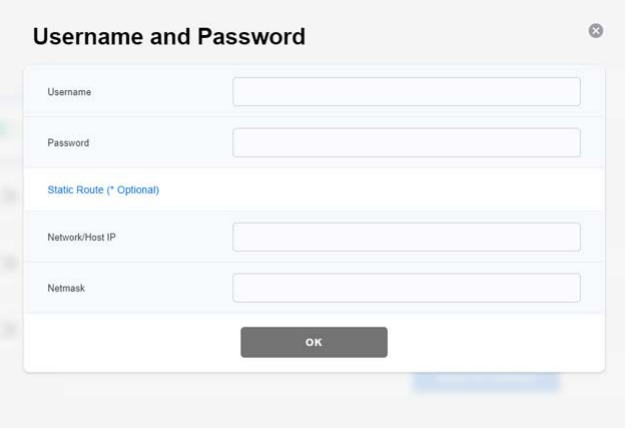
4.16 Server VPN

4.16.1 PPTP

1. Dal pannello di navigazione, andare su **VPN Server (Server VPN)** > **PPTP** e spostare il cursore verso destra (per impostazione predefinita è disattivato sul lato sinistro).
2. Nel campo **VPN Client (Client VPN) (limite max.: 16)**, fare clic su ⊕ per aggiungere un account.



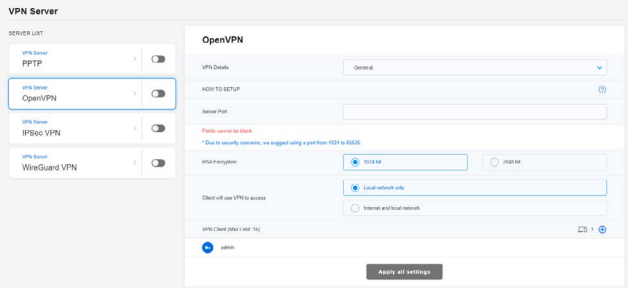
3. Immettere [Nome utente] e [Password] personalizzati e fare clic su **OK**.



NOTA: Una volta impostati, [Nome utente] e [Password] non possono essere modificati. Per altre informazioni, visitare https://www.asus.com/support/FAQ/114892/.

4.16.2 OpenVPN

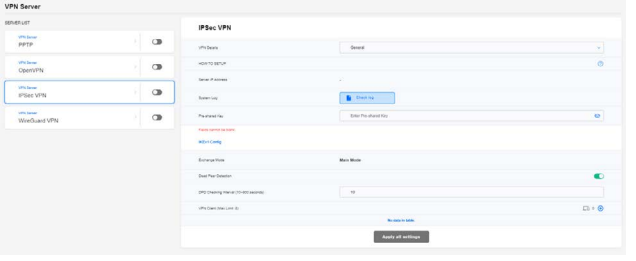
1. Dal pannello di navigazione, andare su **VPN Server (Server VPN)** > **OpenVPN** e spostare il cursore verso destra (per impostazione predefinita è disattivato sul lato sinistro).
2. Configurare le impostazioni generali nel campo **VPN Details (Dettagli VPN)**.
3. Immettere nome utente e password nella colonna vuota.
4. Nel campo **VPN Client (Client VPN) (limite max.: 16)**, fare clic su ⊕ per aggiungere un account.
5. La password viene nascosta automaticamente. Cliccate su **Applica tutte le impostazioni**.



NOTA: Per altre informazioni, visitare https://www.asus.com/support/FAQ/1008713/.

4.16.3 IPSec VPN

1. Dal pannello di navigazione, andare su **VPN Server (Server VPN)** > **IPSec VPN** e spostare il cursore verso destra (per impostazione predefinita è disattivato sul lato sinistro).
2. Immettere una chiave nel campo **Pre-sahred Key (Chiave già condivisa)**.
3. Nel campo **VPN Client (Client VPN) (limite max.: 8)**, fare clic su ⊕ per aggiungere un account.
4. Immettere [Nome utente] e [Password] personalizzati e fare clic su **Apply all settings (Applica tutte le impostazioni)**.

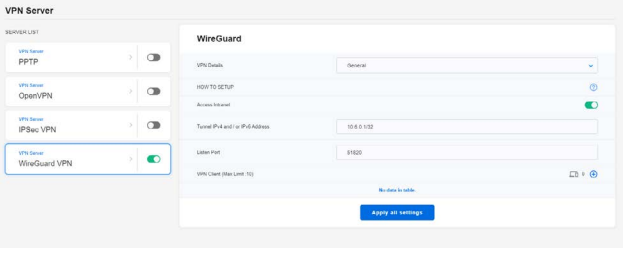


NOTA: Una volta impostati, [Nome utente] e [Password] non possono essere modificati. Per altre informazioni, visitare https://www.asus.com/support/FAQ/1044190/.

4.16.4 VPN WireGuard®

1. Dal pannello di navigazione, andare su **VPN Server (Server VPN)** > **WireGuard VPN (VPN WireGuard)**.
2. Nel campo **VPN Client (Client VPN) (limite max.: 10)**, fare clic su ⊕ per aggiungere un account. Per dispositivi generici come laptop o smartphone, fare clic su **Applica**.
3. Fare clic su **Apply all settings (Applica tutte le impostazioni)** per abilitare la VPN WireGuard®.
4. Per ulteriori informazioni, fare clic su " ••• ".

NOTA: Se si utilizza uno smartphone per connettersi alla VPN WireGuard®, scaricare l'app WireGuard® da Google Play o App Store ed eseguire la scansione del codice nell'app per scaricare il file di configurazione.

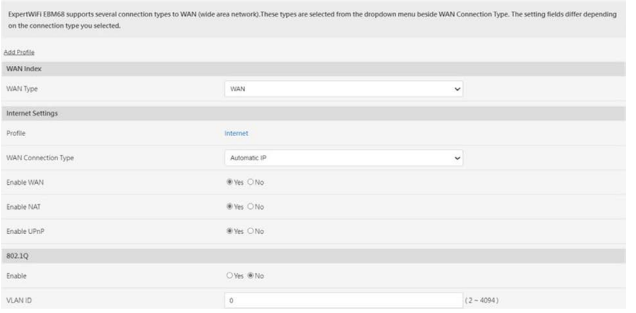


NOTA: Per altre informazioni, visitare https://www.asus.com/support/FAQ/1048280/.

4.17 WAN

4.17.1 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 **Settings (Impostazioni)** > **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. Selezionare **No** per disabilitare l'accesso a Internet.
   - **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.

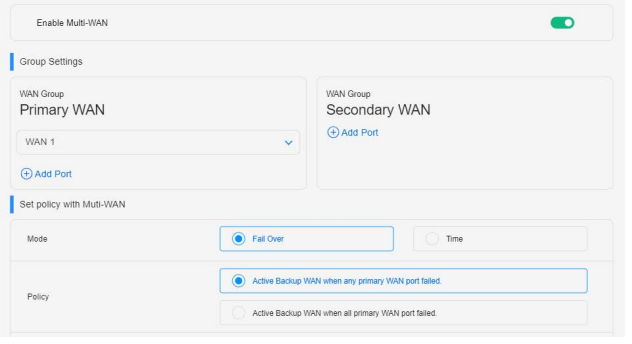
- **Connetti al Server DNS:** Ordina al router di ottenere automaticamente dall'ISP l'indirizzo IP del Server DNS. Un Server DNS è un'entità presente nella rete Internet che si occupa di tradurre gli indirizzi Internet nei corrispondenti indirizzi IP.
- **Autenticazione:** Questo campo potrebbe essere 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 cablato ASUS in modo che sia uguale all'indirizzo MAC del vostro precedente router.

4.17.2 Multi-WAN

Multi-WAN consente di selezionare più connessioni ISP al router e ai gruppi WAN sia per la WAN primaria che per quella secondaria.

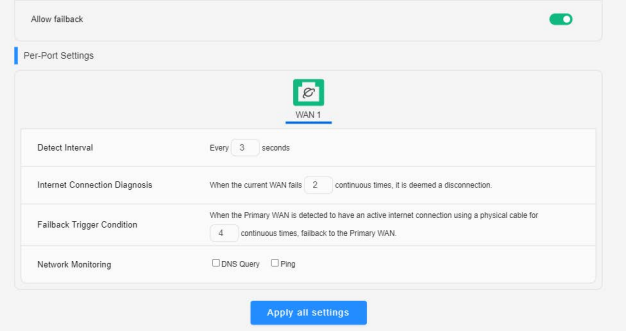
Per configurare Multi-WAN:

1. Dal pannello di navigazione andate su **Settings (Impostazioni)** > **WAN** > **Multi-WAN**.
2. Attivare **Enable Multi-WAN (Abilita Multi-WAN)**.
3. Selezionate la **Primary WAN (WAN primaria)** e la **Secondary WAN (WAN secondaria)**. Le opzioni disponibili sono WAN, USB e Ethernet LAN.
4. Selezionate tra le modalità **Fail Over** o **Time (Ora)**.
   - **Fail Over:** Utilizzare una WAN secondaria per l'accesso alla rete di backup.
   - **Ora:** Impostare l'orario in cui pianificare la policy Multi-WAN.
5. Scegliere **Active Backup WAN when any primary WAN port failed (Backup WAN attivo quando una porta WAN primaria non funziona)** o **Active Backup WAN when all primary WAN port failed (Backup WAN attivo quando tutte le porte WAN primarie non funzionano)**.



6. Attivare o disattivare **Allow failback (Consenti failback)**.

7. Specificare l'intervallo di rilevamento.
8. Specificare il numero di errori continui prima che la WAN attuale venga considerata disconnessa.
9. Specificare il numero di volte continue in cui la WAN primaria viene rilevata come dotata di una connessione Internet attiva tramite un cavo fisico, che attiva un failback sulla WAN primaria.
10. Scegliere **DNS Query (Query DNS)** o **Ping**.
11. Cliccate su **Applica tutte le impostazioni**.



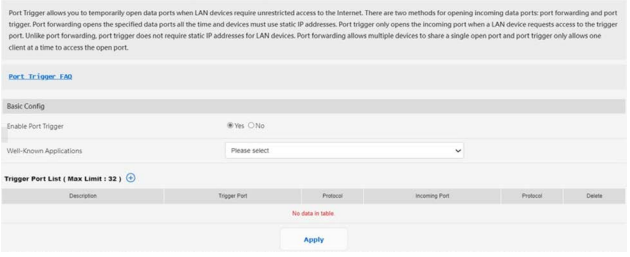
NOTA: Nelle domande frequenti (FAQ) sul sito di supporto ASUS https://www.asus.com/it/support/FAQ/1011719/ potete trovare una spiegazione dettagliata che vi aiuterà ad usare questa funzione in modo adeguato.

4.17.3 Port Trigger

Trigger porta permette di abilitare temporaneamente porte dati quando i dispositivi LAN richiedono l'accesso illimitato ad Internet. Esistono due metodi per aprire le porte dati di ingresso: port forwarding e port triggering.

- Il port forwarding abilita le porte dati specificate per tutto il tempo ed i dispositivi devono usare indirizzi IP statici.
- Il port triggering abilita solo la porta di ingresso quando un dispositivo LAN richiede l'accesso alla porta trigger.

Diversamente dal port forwarding, il trigger porta non necessita di indirizzi IP statici per i dispositivi LAN. Il port forwarding consente a più dispositivi di condividere una singola porta aperta mentre il trigger porta consente ad un solo client alla volta di accedere alla porta aperta.



Per configurare il Port Trigger:

1. Dal pannello di navigazione andate su **Settings (Impostazioni)** > **WAN** > **Port Trigger**.
2. Configurate le seguenti impostazioni. Quando avete finito cliccate su **Apply (Applica)**.
   - **Abilita Port Trigger:** Selezionate Yes (Sì) per abilitare il Port Trigger.
   - **Applicazioni Comuni:** Selezionate giochi e servizi web comuni da aggiungere all'elenco di Port Trigger.
   - **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.

NOTE:

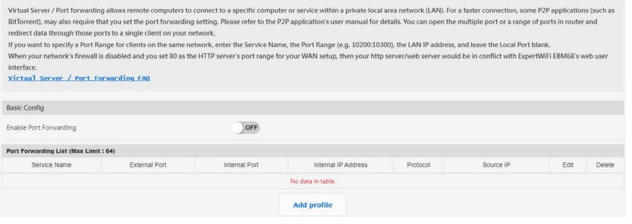
- Quando vi connettete ad un server IRC un PC client stabilisce una connessione in uscita usando l'intervallo di porte trigger 6666-7000. Il server IRC risponde verificando il nome utente e creando una nuova connessione verso il PC client usando una porta in ingresso.
- Se il Port Trigger è disabilitato 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.
- Per altre informazioni, visitare https://www.asus.com/support/FAQ/114110.

4.17.4 Virtual Server/Port Forwarding

Virtual Server/Port forwarding consente ai computer remoti di collegarsi ad un computer o ad un servizio specifico all'interno di una LAN (Local Area Network). Per una connessione più veloce, alcune applicazioni P2P (come BitTorrent), possono anche richiedere di configurare l'impostazione di port forwarding. Fare riferimento al manuale d'uso dell'applicazione P2P per i dettagli. È possibile abilitare nel router porte multiple o un intervallo di porte e reindirizzare i dati attraverso queste porte ad un singolo client sulla rete.

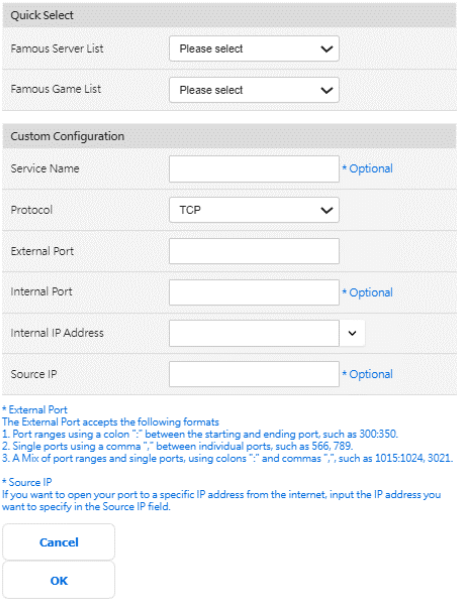
Per specificare un intervallo di porte per i client sulla stessa rete, completare i campi Nome servizio, Intervallo porte (ad esempio, 10200:10300), Indirizzo IP LAN e lasciare vuoto il campo Porta locale.

NOTA: Quando il Port Forwarding è abilitato il router ASUS blocca il traffico non richiesto proveniente da Internet e permette l'ingresso solamente alle risposte relative alle richieste in uscita provenienti dalla LAN. Il client di rete non ha accesso direttamente a Internet e viceversa.



Per configurare il Port Forwarding:

1. Dal pannello di navigazione andate su **Settings (Impostazioni)** > **WAN** > **Virtual Server / Port Forwarding**.
2. Spostate il cursore su **ON** per abilitare il **Port Forwarding**, quindi cliccate su **Add Profile (Aggiungi profilo)**. Dopo aver configurato le impostazioni cliccate su **OK**.



- **Servizi più comuni:** Selezionate il tipo di servizio al quale volete accedere.
- **Giochi più comuni:** Lista dei port forwarding standard per i giochi online più diffusi.
- **Nome del servizio:** Inserite il nome del servizio.
- **Protocollo:** Selezionate il protocollo. Se non siete sicuri selezionate **BOTH (ENTRAMBI)**.
- **Porta esterna:** Accetta i seguenti formati:

  1) Un intervallo di porte può essere specificato usando i due punti ":" tra la porta iniziale e la porta finale, ad esempio 300:350;

  2) Porte singole possono essere specificate usando una virgola "," per separare una porta dall'altra, ad esempio 566, 789;

  3) Il sistema accetta anche un misto tra intervalli di porte e porte singole, l'utente può usare i due punti ":" e le virgole ",", ad esempio 1015:1024, 3021.
- **Porta interna:** 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.

- **Indirizzo IP interna:** Inserite l'indirizzo IP locale del client.
- **IP sorgente:** Se volete aprire una porta per un indirizzo IP Internet specifico inserite l'indirizzo IP al quale volete dare accesso in questo campo.

NOTA: Assicuratevi che il client disponga di un indirizzo IP statico per fare in modo che il port-forwarding funzioni correttamente. Fate riferimento alla sezione *4.9 LAN* per maggiori informazioni.

Per controllare che il Port Forwarding sia configurato correttamente:

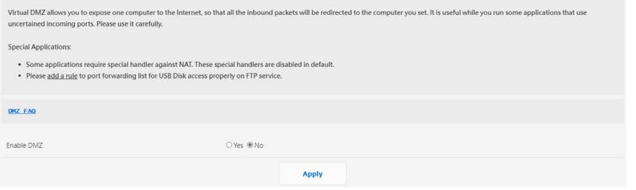
- Assicuratevi che il vostro server, o l'applicazione, siano avviati e operativi.
- Avete bisogno di un client al di fuori della vostra rete LAN (Internet client). Questo client non deve essere connesso al router ASUS.
- Dall'Internet client usate l'indirizzo IP pubblico (WAN) del router per accedere 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.

4.17.5 DMZ

DMZ virtuale consente di esporre un computer ad Internet, in modo che tutti i pacchetti in ingresso saranno reindirizzati al computer impostato. È utile durante l'esecuzione di alcune applicazioni che usano porte in ingresso incerte. Utilizzare con cura.



Per configurare DMZ:

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

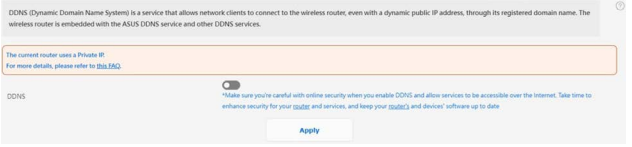
Per disabilitare DMZ:

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)**.

NOTA: Per altre informazioni, visitare https://www.asus.com/support/FAQ/1011723.

4.17.6 DDNS

DDNS (Dynamic Domain Name System) è un servizio che consente ai client di rete di connettersi al router cablato, anche con un indirizzo IP pubblico dinamico, mediante il relativo nome di dominio registrato. Il router cablato è integrato con il servizio DDNS ASUS e altri servizi DDNS.



Per configurare un DNS Dinamico:

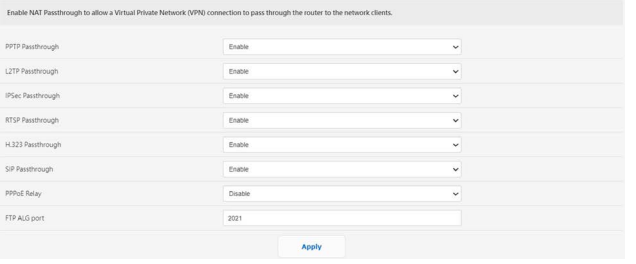
1. Dal pannello di navigazione andate su **Settings (Impostazioni)** > **WAN** > **DDNS**.
2. Configurate le seguenti impostazioni. Quando avete finito cliccate su **Apply (Applica)**.
   - **Enable the DDNS Client (Abilita il client DDNS):** Abilita l'accesso al router ASUS dall'esterno tramite nome 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 **User Name (Nome utente)** o **E-mail Address and Password (Indirizzo email e Password)** o **DDNS Key (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 cablato usa come indirizzo pubblico (WAN) un indirizzo IP destinato alle reti private (192.168.x.x, 10.x.x.x, o 172.16.x.x) come indicato dalla scritta in giallo.
- Il router si trova in una rete che usa NAT multipli.

4.17.7 NAT Passthrough

Abilitare Passthrough NAT per consentire ad una connessione VPN (Virtual Private Network) di passare attraverso il router per raggiungere i client di rete.

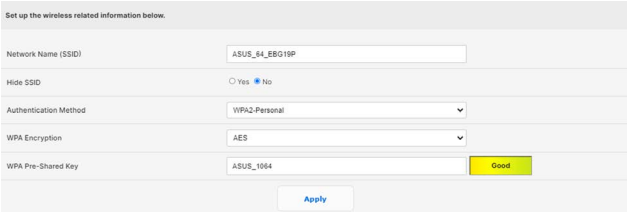
Per configurare Passthrough NAT, andare su **Settings (Impostazioni)** > **WAN** > **NAT Passthrough**. Quando avete finito cliccate su **Apply (Applica)**.



4.18 Wireless

4.18.1 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 **Settings (Impostazioni)** > **Wireless** > **General (Generale)**.
2. Assegnare un nome univoco all'SSID (Service Set Identifier) o un nome di rete per identificare la 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.

   IMPORTANTE!Per rendere disponibile la funzione Wi-Fi, assicurarsi di integrare un punto di accesso wireless (AP) come ExpertWiFi EBA63 o un router come ExpertWiFi EBR63 o ExpertWiFi EBM68 nella rete AiMesh dell'EBG19P.

   ---

3. 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.
4. Selezionate uno di questi metodi di autenticazione:
   - **Sistema aperto:** Questa opzione non fornisce sicurezza.
   - **WPA/WPA2/WPA3-Personal:** Questa opzione fornisce un elevato livello di sicurezza. Potete scegliere di usare WPA (TKIP) o WPA2 (AES). Se scegliete questa opzione

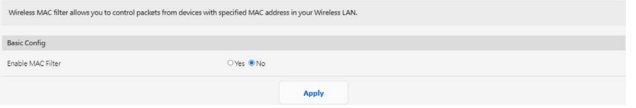
dovete usare la cifratura TKIP o AES e inserire una passphrase WPA (chiave di rete).

- **WPA/WPA2/WPA3-Enterprise:** Questa opzione fornisce un livello molto elevato di sicurezza. È previsto un server di autenticazione che può essere integrato (EAP) o esterno (RADIUS).

5. Assegnare una password univoca per la chiave precondivisa WPA.

4.18.2 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.

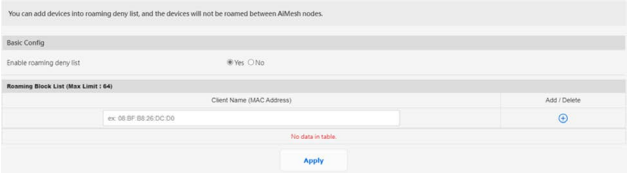


Per impostare il Filtro MAC wireless:

1. Dal pannello di navigazione andate su **Settings (Impostazioni)** > **Wireless** > **Wireless MAC Filter (Filtro MAC Wireless)**.
2. Alla voce **Enable MAC Filter (Abilita filtro MAC)** selezionate **Yes (Sì)**.
3. Nel menu **MAC Filter Mode (Modalità filtro MAC)** selezionate **Accept (Accetta)** o **Reject (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.
4. In **Elenco filtro MAC** cliccate su ⊕ e inserite l'indirizzo MAC del dispositivo wireless.
5. Cliccate su **Apply (Applica)**.

4.18.3 Elenco dei blocchi di roaming

La funzione consente di aggiungere dispositivi all'elenco dei blocchi di roaming e impedire loro il roaming tra i nodi AiMesh.



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/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. Dal pannello di navigazione andate su **Settings (Impostazioni)** > **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 per ottenere il firmware aggiornato.
3. Dalla pagina **Firmware Upgrade (Aggiornamento firmware)** cliccate su **Browse (Sfoglia)** per caricare 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.

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 cablato 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 **Dashboard** > **Clients (Client)**.

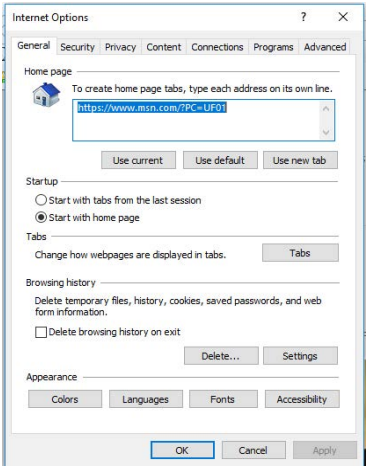
5.2 Domande e risposte frequenti (FAQs)

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. 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 **General (Generale)**, sotto **Browsing history (Cronologia esplorazioni)**, fare clic su **Delete… (Elimina…)**, selezionare **Temporary Internet files and website files (File temporanei Internet e file di siti Web)** e **Cookies and website data (Cookie e dati di siti Web)**, quindi fare clic su **Delete (Elimina)**.



NOTE:

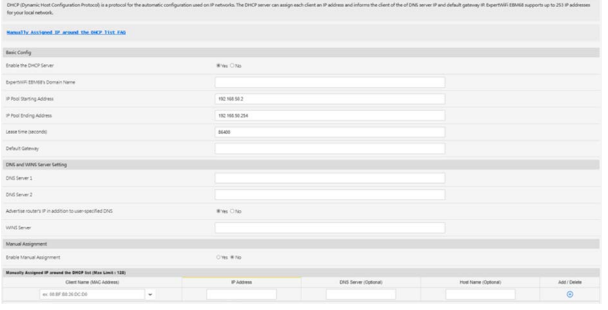
- La procedura per la rimozione dei cookie e dei file temporanei potrebbe variare a seconda del browser utilizzato.
- Disabilitate il server proxy, le connessioni remote e configurate le impostazioni TCP/IP in modo da ottenere un indirizzo IP automaticamente. Per maggiori informazioni fate riferimento 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.

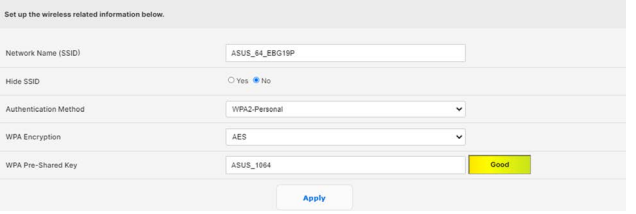
IMPORTANTE! Per rendere disponibile la funzione Wi-Fi, assicurarsi di integrare un punto di accesso wireless (AP) come ExpertWiFi EBA63 o un router come ExpertWiFi EBR63 o ExpertWiFi EBM68 nella rete AiMesh dell'EBG19P.

- Il server DHCP è stato disabilitato:

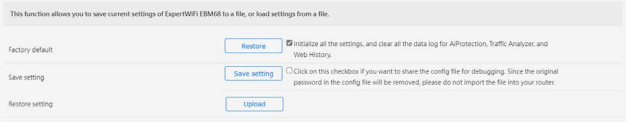
  1. Aprite l'interfaccia web. Andate su **Dashboard** > **Clients (Client)** e cercate il dispositivo che volete connettere al router.
  2. Se non riuscite a trovare il dispositivo nella **Dashboard** andate su **Settings (Impostazioni)** > **LAN** > **DHCP Server (Server DHCP)**.



- 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 **Settings (Impostazioni)** > **Wireless** > **General (Generale)**, selezionate **NO** alla voce **Hide SSID (Nascondi SSID)**.



- 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 si riesce a connettersi al router via cavo, potete resettare il router alle impostazioni predefinite di fabbrica. Aprite l'interfaccia web, andate su **Settings (Impostazioni)** >**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 **Dashboard** e controllate la voce Internet Status (Stato Internet).
- Se il tuo router non riesce a connettersi all'indirizzo IP WAN del tuo ISP, prova a riavviare la rete come descritto nella sezione **Restart your network in the following sequence (Riavvia la rete nella seguente sequenza)** sotto **Basic Troubleshooting (Risoluzione dei problemi di base)**.

- 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 cablato. Se il LED WAN sul cablato 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 **Dashboard**, 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 **Settings (Impostazioni)** > **Administration (Amministrazione)** > **Restore/Save/Upload Setting (Impostazione Ripristina/Salva/Carica)** e cliccate sul pulsante **Restore (Ripristina)**.

Come faccio a ripristinare le impostazioni predefinite del router?

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

Aggiornamento del firmware non riuscito.

Lanciate la modalità di recupero e eseguite l'utility **Firmware Restoration (Ripristino del firmware)**.

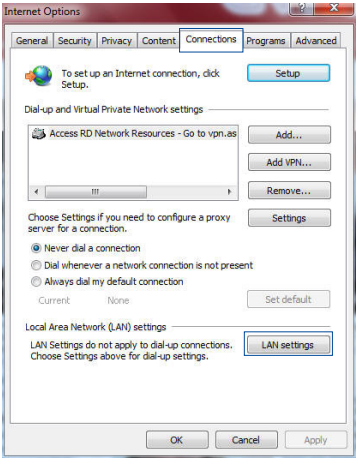
Impossibile accedere all'interfaccia web

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

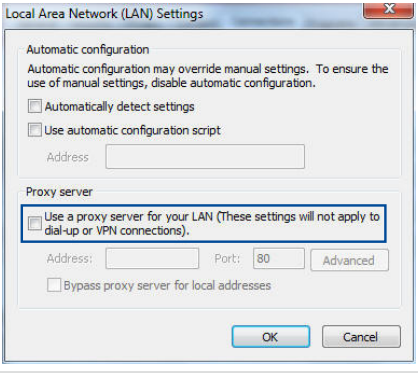
A. Disabilitate il server proxy (se abilitato).

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)**.

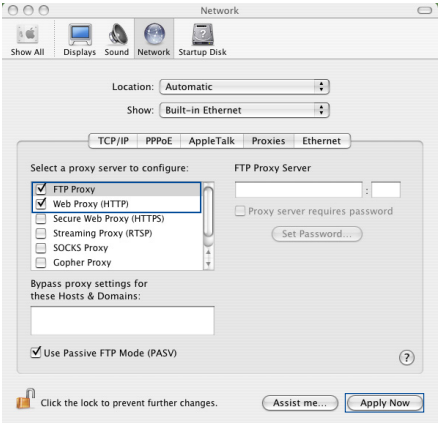


3. Dalla schermata di impostazioni della vostra LAN (Local Area Network) togliete la spunta da **Use a proxy server for your LAN (Utilizza un proxy server per le connessioni LAN)**.
4. Quando avete finito selezionate **OK**.



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)**.

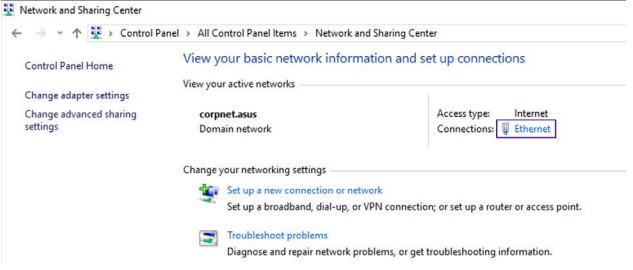


NOTA: Fate riferimento alla funzione *Aiuto* del vostro browser per dettagli su come disabilitare una connessione remota.

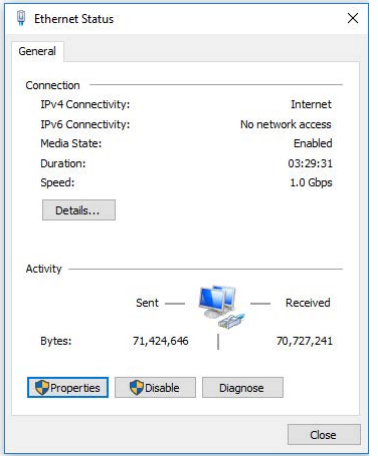
B. Configurate le impostazioni TCP/IP in modo da ottenere un indirizzo IP automaticamente.

Windows®

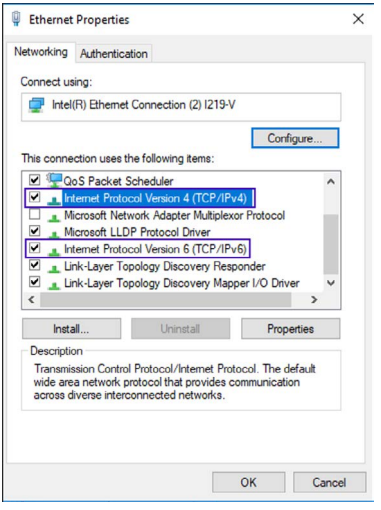
1. Cliccate su **Start** > **Control Panel (Pannello di controllo)** > **Network and Sharing Center (Centro connessioni di rete e condivisione)** quindi cliccate sulla connessione di rete per visualizzare la finestra di stato.



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



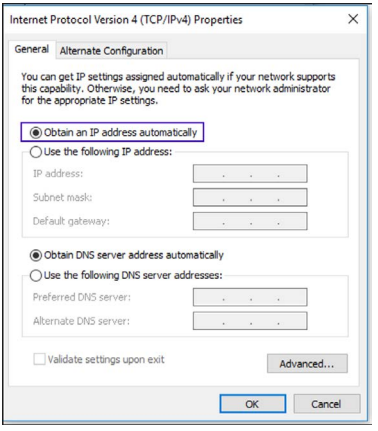
3. Selezionate **Protocollo Internet versione 4 (TCP/IPv4)** o **Internet Protocol Version 6 (TCP/IPv6) (Protocollo Internet versione 6 (TCP/IPv6))** e poi cliccate su Proprietà.



4. Per ottenere automaticamente le impostazioni IPv4 selezionate **Obtain an IP address automatically (Ottieni automaticamente un indirizzo IP)**.

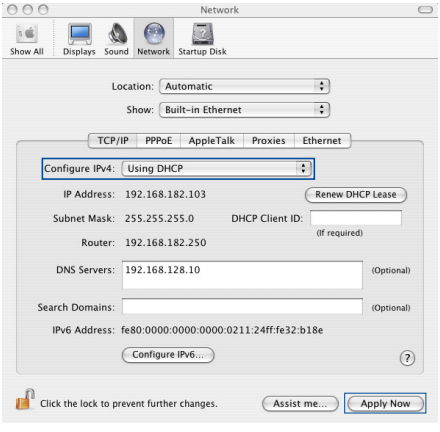
Per ottenere automaticamente le impostazioni IPv6 selezionate **Obtain an IPv6 address automatically (Ottieni automaticamente un indirizzo IPv6)**.

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



MAC OS

1. Cliccate sull'icona della mela sulla parte in alto a sinistra 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)**.

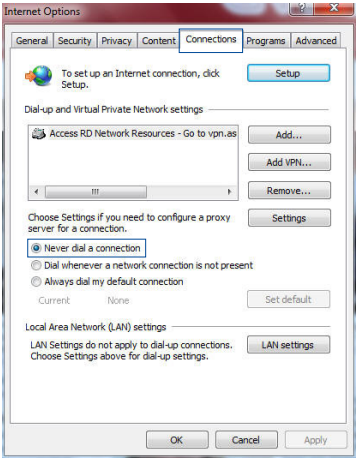


NOTA: Fate riferimento alle informazioni su aiuto e supporto del vostro sistema operativo per avere maggiori dettagli sulla configurazione delle impostazioni TCP/IP del vostro computer.

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 montare questa apparecchiatura a un'altezza superiore a 2 metri.
- Usa questo prodotto in ambienti la cui temperatura sia compresa tra 0℃ (32˚F) e 40℃ (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.
- Il prodotto è solo per l’uso all’interno.

Avviso WEEE

La Direttiva sui rifiuti di apparecchiature elettriche ed elettroniche (WEEE) (Direttiva 2012/19/UE) è una normativa dell'Unione Europea che mira a ridurre l'impatto ambientale delle apparecchiature elettriche ed elettroniche. Obbliga i produttori a prendersi la responsabilità della gestione del fine vita dei loro prodotti, promuovendo la raccolta, il trattamento e il riciclaggio per ridurre al minimo i rifiuti e favorire il recupero delle risorse.

Non smaltire le apparecchiature elettroniche ed elettriche insieme ai rifiuti urbani.

Il simbolo del bidone dei rifiuti barrato da una croce sul prodotto o sull'imballaggio indica che questo prodotto (comprese eventuali batterie in esso contenute) non deve essere smaltito insieme ai normali rifiuti domestici.

Per prevenire potenziali danni all'ambiente e alla salute umana, è necessario utilizzare un sistema di raccolta per restituire, riciclare e recuperare i rifiuti di apparecchiature elettriche ed elettroniche (RAEE). Questo prodotto è stato progettato per consentire il riutilizzo di alcune parti e facilitare il riciclaggio di determinati materiali.

Lo smaltimento improprio può comportare rischi a causa della presenza di sostanze pericolose all'interno delle apparecchiature elettriche ed elettroniche, come il piombo, i BFR e altri componenti dannosi.

Controlla i servizi locali di riciclaggio per i prodotti elettronici (https://esg.asus.com/en/circular-economy/resource-regeneration/global-take-back-service).