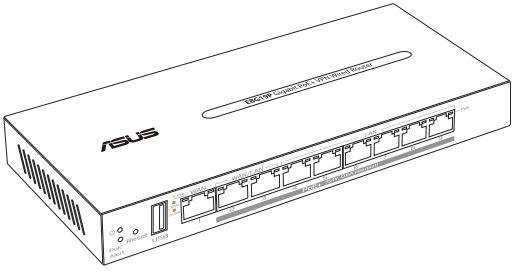
Manual do utilizador

ASUS EBG19P

Router PoE+ VPN Gigabit com fios

Modelo: EBG19P



ASUS
IN SEARCH OF INCREDIBLE

PG23436
Primeira edição
Maio de 2024

Índice

Índice

Índice

1 Conheça o seu EBG19P

1.1 Bem-vindo!

Obrigado por ter adquirir um Router Sem Fios ASUS EBG19P!

O EBG19P fornece uma rede rápida, segura e dimensionável, estabilidade de rede melhorada através de ligação Ethernet e cópia de segurança na Internet com duas portas WAN/LAN e uma porta USB para suportar as operações.

1.2 Conteúdo da embalagem

- ☑ EBG19P
- ☑ Transformador
- ☑ Guia de consulta rápida
- ☑ Cabo de rede (RJ-45)
- ☑ Adesivo de informações de início de sessão local
- ☑ Cartão de Garantia

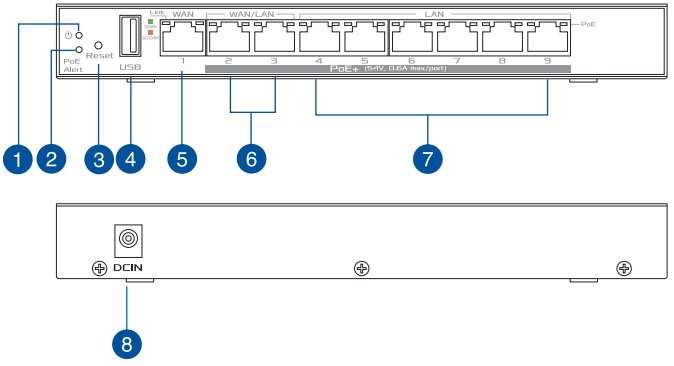
NOTAS:

- Se algum dos itens estiver danificado ou em falta, contacte a ASUS. Para questões técnicas e apoio, consulte **Service and Support (Assistência E Suporte)** na traseira deste manual do utilizador.
- Guarde a embalagem original, para a eventualidade de serem necessários futuros serviços de assistência em garantia, tais como reparação ou substituição do produto.

1.3 O seu router com fios

1. Ligue o transformador à porta de entrada DC.
2. O LED de energia irá acender quando o aparelho estiver preparado.

Descrição dos botões e portas



1	**LED de alimentação** **Desligado:** Sem alimentação. **Ligado:** O dispositivo está preparado. **Intermitente lento:** Modo de recuperação
2	**LED de alerta PoE** **Desligado:** Sem alimentação ou ligação física. **Ligado:** Está a ser fornecida energia a um dispositivo ligado à porta PoE+.
3	**Botão de reposição** Este botão repõe ou restaura as predefinições do sistema.
4	**Porta USB 3.2 Gen 1** Insira nesta porta um dispositivo com USB 3.2 Gen 1, como um disco rígido USB ou uma unidade flash USB.
5	**Porta WAN (Internet)** Ligue um cabo de rede a esta porta para estabelecer a ligação WAN.
6	**Portas WAN / LAN (com PoE+)** Ligue um cabo de rede a esta porta para estabelecer a ligação WAN / LAN.
7	**Portas LAN (com PoE+)** Ligue o seu PC a esta porta LAN com um cabo de rede.
8	**Porta de alimentação (Entrada DCIN)** Ligue o transformador AC fornecido a esta porta e ligue o router a uma tomada eléctrica.

Indicações LED da porta de Ethernet

Indicadores LED			
LED de velocidade (Verde)		LED de ligação/atividade (Âmbar)	
Ligação de 1 Gbps	ATIVADO	Ligação de 1 Gbps / 100 Mbps / 10 Mbps	Intermitente
Ligação de 100 Mbps / 10 Mbps	DESATIVADO	Sem tráfego	ATIVADO

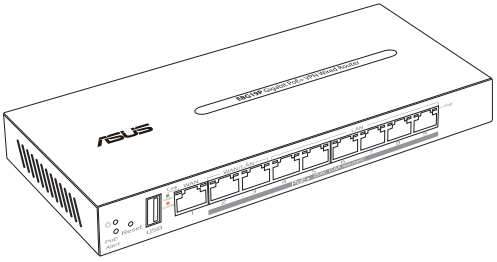
Especificações:

Transformador DC	Saída DC: +54V com corrente máx. de 2.778A		
Temperatura de funcionamento	0 a 40°C	Armazenamento	0 a 70°C
Humidade em funcionamento	50 a 90%	Armazenamento	20 a 90%

1.4 Colocação do router

Para a melhor experiência de ligação à rede, certifique-se de que:

- Actualize sempre para o firmware mais recente. Visite o Web site da ASUS em **http://www.asus.com** para obter as actualizações de firmware mais recentes.



1.5 Requisitos de configuração

Para configurar a sua rede, precisa de um computador que cumpram os seguintes requisitos:

- Porta Ethernet RJ-45 (LAN) (10Base-T/100Base-TX/1000BaseTX)
- Um serviço TCP/IP instalado
- Navegador Web, como por exemplo o Internet Explorer, Firefox, Safari ou o Google Chrome

NOTA: Os cabos Ethernet RJ-45 utilizados para ligar os dispositivos de rede não deverão exceder 100 metros de comprimento.

1.6 Configuração do router

IMPORTANTE!

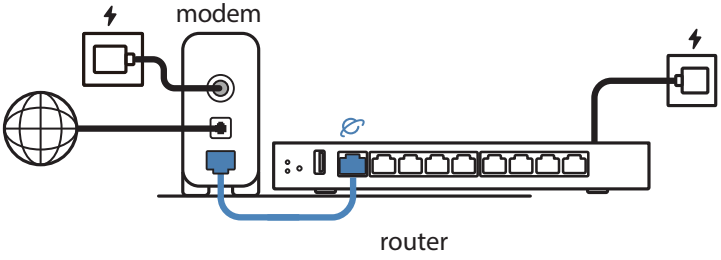
- Antes de configurar o seu router com fios ASUS, faça o seguinte:
  - Se estiver a substituir um router, desligue-o da sua rede.
  - Desligue os cabos/fios ligados ao modem. Se o modem possuir uma bateria de reserva, remova-a também.
  - Reinicie o computador (recomendado).

AVISO!

- O(s) cabo(s) de alimentação deve(m) ser ligado(s) a tomadas elétricas com ligação à terra adequada. Ligue o equipamento apenas a uma tomada elétrica próxima e facilmente acessível.
- Se a fonte de alimentação estiver avariada, não tente repará-la por si próprio. Contacte um técnico qualificado ou o seu revendedor.
- NÃO utilize cabos de alimentação, acessórios ou outros periféricos danificados.
- NÃO instale este equipamento a uma altura superior a 2 metros.
- Utilize este equipamento em ambientes com temperaturas entre 0˚C (32˚F) e 40˚C (104˚F).

1.6.1 Ligação com fios

NOTA: O router sem fios integra uma função de cruzamento automático, isto permite-lhe utilizar quer um cabo simples quer um cabo cruzado para a ligação com fios.



Para configurar o router com fios através de uma ligação com fios:

1. Ligue o transformador AC do router com fios à porta de entrada DC e a uma tomada eléctrica.
2. Utilizando o cabo de rede fornecido, ligue o seu computador à porta LAN do router com fios.
3 Utilizando outro cabo de rede, ligue o seu modem à porta WAN do router com fios.
4. Ligue o transformador AC do modem à porta de entrada DC e a uma tomada eléctrica.

2 Começar a utilizar

2.1 Iniciar sessão na GUI Web

O seu router com fios ASUS oferece uma interface gráfica Web (GUI) intuitiva que permite configurar facilmente as várias funções através de um navegador Web, como o Microsoft Edge, Safari ou o Google Chrome.

NOTA: As funcionalidades poderão variar de acordo com as diferentes versões de firmware.

Ligar à sua rede acesso com cabo:

Para iniciar sessão na GUI Web:

1. No seu navegador Web, introduza http://expertwifi.net.
2. Siga as instruções de configuração.

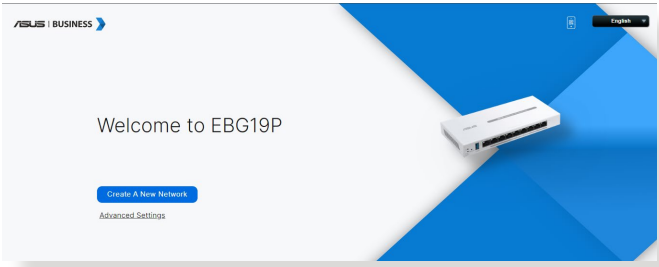
2.2 Deteção automática de WAN

A função de Configuração Rápida de Internet (QIS) ajuda a configurar rapidamente a sua ligação à Internet.

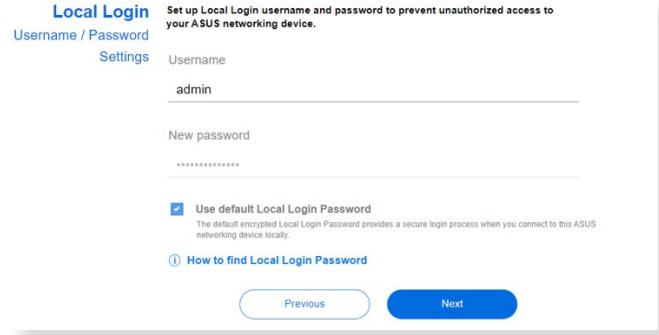
NOTA: Quando configurar a ligação à Internet pela primeira vez, prima botão de reposição no router com fios para repor as predefinições.

Deteção automática de WAN:

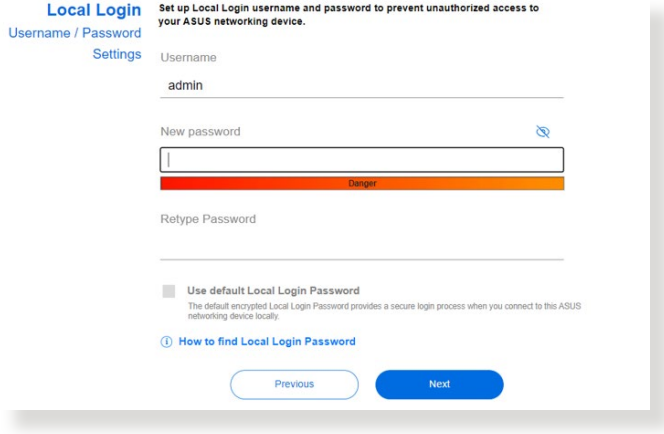
1. Inicie sessão na Interface Web e clique em **Create A New Network (Criar uma rede nova)**.



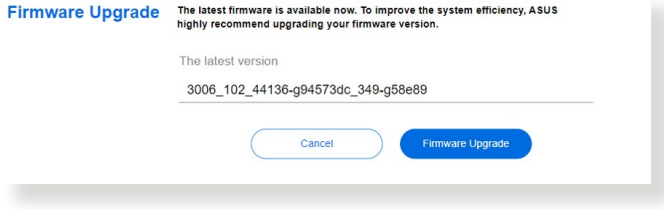
2. Clique em **Next (Seguinte)** para iniciar sessão com o nome de utilizador e a palavra-passe.



Desmarque a opção **Use default Local Login Password (Utilizar palavra-passe de início de sessão local predefinida)**, e introduza um nome de utilizador e palavra-passe novos. Em seguida, clique em **Next (Seguinte)**.



3. Clique em **Firmware Upgrade (Atualização de firmware)** para atualizar o firmware para a versão mais recente ou clique em **Cancel (Cancelar)** para manter a versão atual.



NOTA: O ecrã é apresentado apenas quando está disponível uma nova versão do firmware.

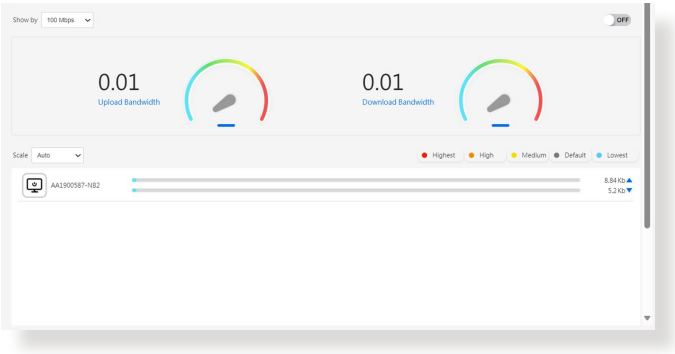
3 Configurar EBG19P

3.1 QoS Adaptativo

3.1.1 Monitor de Largura de Banda

O Monitor de Largura de Banda permite monitorizar a utilização da largura de banda de transferência e envio total e de cada cliente.

Para utilizar o **Bandwidth Monitor (Monitor de Largura de Banda)**, aceda a **Settings (Definições)** > **Adaptive QoS (QoS Adaptativo)** > **Bandwidth Monitor (Monitor de Largura de Banda)**.

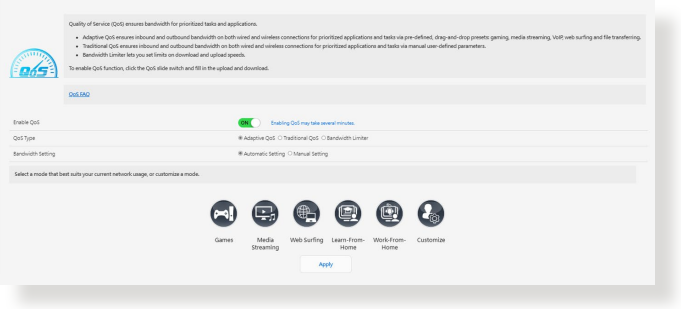


NOTA: Para mais informações, visite https://www.asus.com/support/faq/1008717.

3.1.2 QoS

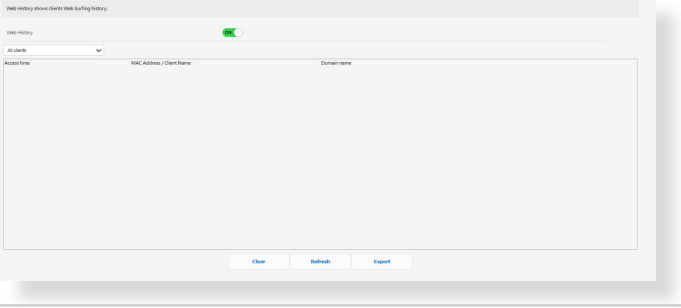
A Qualidade de Serviço (QoS) garante uma largura de banda para tarefas e aplicações prioritárias.

1. O **Adaptive QoS (QoS Adaptativo)** garante largura de banda de entrada e saída em ligações com e sem fios para aplicações e tarefas prioritárias através de predefinições que podem ser arrastadas e largadas: jogos, transmissão de multimédia, VoIP, navegação na Web e transferência de ficheiros.
2. O **Traditional QoS (QoS Tradicional)** disponibiliza uma largura de banda de entrada e saída adequada para ligações com e sem fios para aplicações e tarefas prioritárias através de parâmetros definidos manualmente pelo utilizador.
3. O **Bandwidth Limiter (Limitador de Largura de Banda)** permite definir limites para as velocidades de transferência e de envio.



3.1.3 Histórico da Web

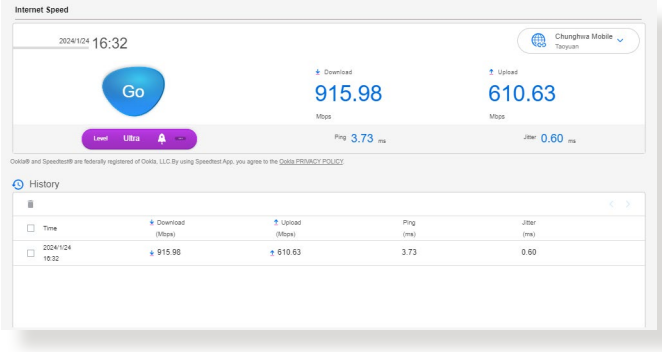
A página **Web History (Histórico da Web)** apresenta o histórico de navegação dos clientes na Web.



3.1.4 Velocidade da Internet

Este serviço é fornecido pela Ookla®. Deteta a velocidade de transferência e envio do seu router à Internet.

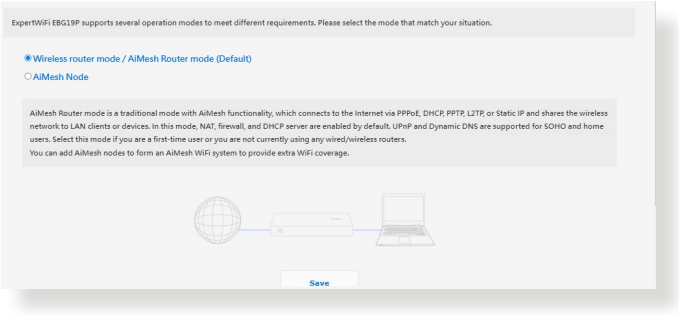
Clique em **GO (INICIAR)** para efetuar um teste de velocidade da Internet, que demora cerca de um minuto a concluir.



3.2 Administração

3.2.1 Modo de Funcionamento

A página Operation Mode (Modo de Funcionamento) permite-lhe selecionar o modo apropriado para a sua rede.



Para configurar o modo de funcionamento:

1. No painel de navegação, aceda a **Settings** (**Definições**) > **Administration (Administração)** > **Operation Mode (Modo de funcionamento)**.
2. Selecione um dos seguintes modos de funcionamento:
   - **Wireless router mode / AiMesh Router mode (Default) (Modo de router sem fios / Modo Router AiMesh (Predefinido))**: O modo Router AiMesh é um modo tradicional com funcionalidade AiMesh que liga à Internet através de PPPoE, DHCP, PPTP, L2TP ou IP estático e partilha a rede sem fios com clientes ou dispositivos na LAN. Neste modo, os serviços de NAT, firewall e servidor DHCP estão ativados por predefinição. Os serviços UPnP e Dynamic DNS são suportados para utilizadores domésticos e de pequenos escritórios.
   - **AiMesh Node (Nó AiMesh)**: Pode adicionar nós AiMesh para formar um sistema WiFi AiMesh para fornecer cobertura Wi-Fi adicional.
3. Clique em **Save (Guardar)**.

NOTA: O router irá reiniciar após a mudança de modo.

3.2.2 Sistema

A página **System (Sistema)** permite-lhe configurar as definições do seu router com fios.

Para configurar as definições do sistema:

1. No painel de navegação, aceda a **Settings (Definições)** > **Administration (Administração)** > **System (Sistema)**.
2. Pode configurar as seguintes definições:
   - **Alterar a palavra-passe de início de sessão do router**: Pode alterar a palavra-passe e o nome de início de sessão do router com fios introduzindo um novo nome e palavra-passe.
   - **USB setting (Configuração USB):** Pode ativar a hibernação de HDD e alterar o modo USB.
   - **Fuso horário:** Selecione o fuso horário da sua rede.
   - **Servidor NTP**: O router com fios pode aceder a um servidor NTP (Protocolo de Hora de Rede) para sincronizar a hora.
   - **Network Monitoring (Monitorização de rede):** Pode ativar a Consulta de DNS para verificar Resolver nome do anfitrião e Endereços IP resolvidos, ou ativar Ping, e verificar o Destino de Ping.
   - **Auto Logout (Terminar sessão automaticamente):** Pode definir a hora para terminar sessão automaticamente.
   - **Enable WAN down browser redirect notice (Ativar aviso de redireccionamento do navegador para WAN desligada):** Esta funcionalidade permite que o navegador exiba uma página de aviso quando o router estiver desligado da Internet. Quando estiver desativada, a página de aviso não será exibida.
   - **Ativar Telnet**: Clique em **Yes (Sim)** para Ativar os serviços Telnet na rede. Clique em **No (Não)** para desativar o serviço Telnet.
   - **Método de autenticação**: Pode seleccionar HTTP, HTTPS ou ambos os protocolos para proteger o acesso ao router.
   - **Enable Reboot Scheduler (Ativar agendamento de reinício):** Quando esta funcionalidade estiver ativada, poderá definir a data para reiniciar e a hora para reiniciar.
   - **Ativar acesso Web a partir da WAN**: Selecione **Yes (Sim)** para permitir que dispositivos fora da rede acedam às definições da interface do utilizador do router com fios. Selecione **No (Não)** para impedir o acesso.

- **Enable Access Restrictions (Ativar restrições de acesso)**: Clique em **Yes (Sim)** se deseja especificar os endereços IP dos dispositivos aos quais é permitido o acesso às definições da interface do utilizador do router com fios a partir da WAN/LAN.
- **Service (Serviço):** Esta funcionalidade permite configurar as definições Ativar Telnet/Ativar porta SSH/SSH/Permitir início de sessão com palavra-passe/Chaves autorizadas/Tempo limite de inatividade.

3. Clique em **Apply (Aplicar)**.

3.2.3 Actualização do firmware

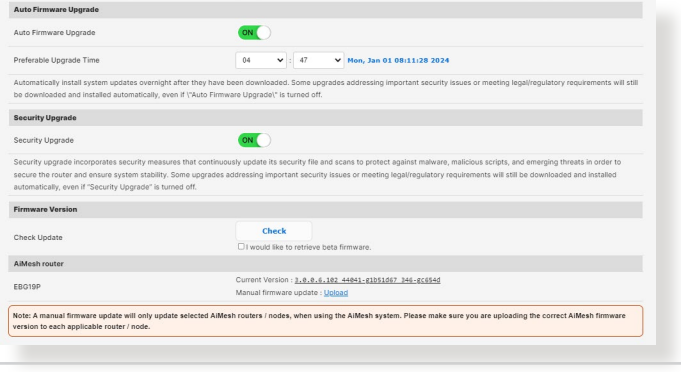
NOTA: Transfira o mais recente firmware a partir do web site da ASUS em **http://www.asus.com.**

Para atualizar o firmware:

1. No painel de navegação, aceda a **Settings (Definições)** > **Administration (Administração)** > **Firmware Upgrade (Atualização do firmware)**.
2. No campo **New Firmware File (Ficheiro de novo firmware)**, clique em **Browse (Procurar)** para localizar o ficheiro transferido.
3. Clique em **Upload (Transferir).**

NOTAS:

- Quando o processo de atualização estiver concluído, aguarde alguns instantes para que o sistema reinicie.
- Se a atualização falhar, o router com fios entra automaticamente no modo de emergência ou de falha e o LED indicador de alimentação existente no painel frontal começa a piscar lentamente.

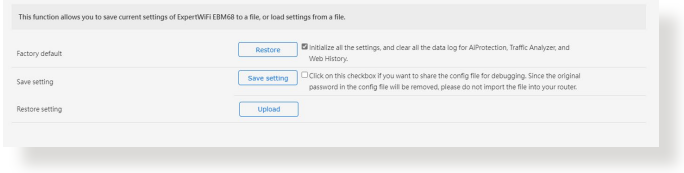


3.2.4 Restaurar/Guardar/Transferir as definições

Para restaurar/guardar/transferir as definições do router com fios:

1. No painel de navegação, aceda a **Settings (Definições)** > **Administration (Administração)** > **Restore/Save/Upload Setting (Restaurar/Guardar/Carregar a Configuração)**.
2. Selecione as tarefas que pretende executar:
   - **Factory default** (**Predefinição de fábrica)**: Inicializa todas as definições e limpa todos os registos de dados de AiProtection, do Analisador de tráfego e do Histórico da Web.
   - **Save setting** (**Guardar configuração)**: Marque esta caixa se pretender partilhar o ficheiro de configuração para depuração. Visto que a palavra-passe original no ficheiro de configuração será removida, não importe o ficheiro para o seu router.
   - **Restore setting (Restaurar configuração)**: Carregue as definições de restauro que pretende aplicar.

IMPORTANTE! Caso ocorram problemas, carregue a versão mais recente do firmware e configure as novas definições. Não restaure as predefinições do router.



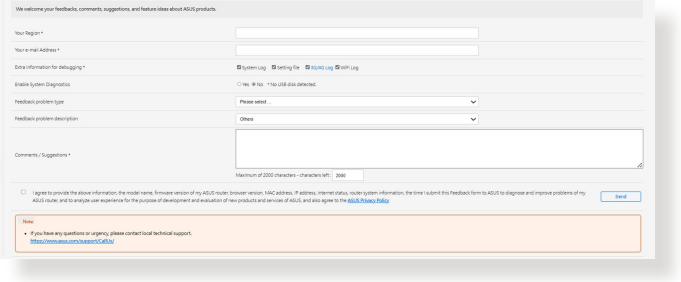
3.2.5 Feedback

Para utilizar o Feedback:

1. No painel de navegação, aceda a **Settings (Definições)** > **Administration (Administração)** > **Feedback**.
2. Introduza a sua região, o endereço de e-mail, informações adicionais para depuração, comentários e sugestões e envie o registo do router para resolução de problemas.

IMPORTANTE!

- Descreva detalhadamente a situação para obter uma resposta rápida.
- Aceite a Política de Privacidade da ASUS.



3.2.6 Privacidade

1. Para vinculação de contas, DDNS e ligação remota (aplicação ASUS Router/Aplicação Lyra/AiCloud/AiDisk):

Tenha em atenção que as suas informações, incluindo o nome do modelo do produto, a versão do firmware, o estado da Internet, o endereço IP, o endereço MAC e o nome de DDNS, serão recolhidas pela ASUS através das funções acima referidas.

Se pretender desativar a partilha das suas informações com a ASUS através das funções acima referidas, clique em **Withdraw (Retirar)** abaixo. No entanto, estas funções podem não funcionar se deixar de partilhar as suas informações com a ASUS.

IMPORTANTE!

- Depois de clicar em **Withdraw (Retirar)**, ocorrerão algumas alterações, conforme indicado abaixo:
  - O nome de DDNS que está a utilizar atualmente não será guardado no seu router.
  - As aplicações ASUS Router, Lyra, AiCloud e AiDisk podem ser utilizadas apenas quando o dispositivo se encontra na mesma rede do router.

2. Aviso de PRIVACIDADE DA ASUS (para atualização de firmware/segurança):

Tenha em atenção que as suas informações serão recolhidas pelo router ASUS para efeitos de atualização de firmware/segurança. Se pretender desativar a partilha das suas informações com o router ASUS, clique em **Withdraw (Retirar)** abaixo.

IMPORTANTE! Clicar em **Withdraw (Retirar)** aqui poderá originar uma falha da atualização para o firmware mais recente e na obtenção da proteção mais atualizada para o seu router ASUS. No entanto, para proteger o seu router e garantir a conformidade com a legislação, as atualizações que abordam aspetos de segurança importantes ou que cumpram requisitos legais/regulamentares continuarão a ser transferidas e instaladas automaticamente.

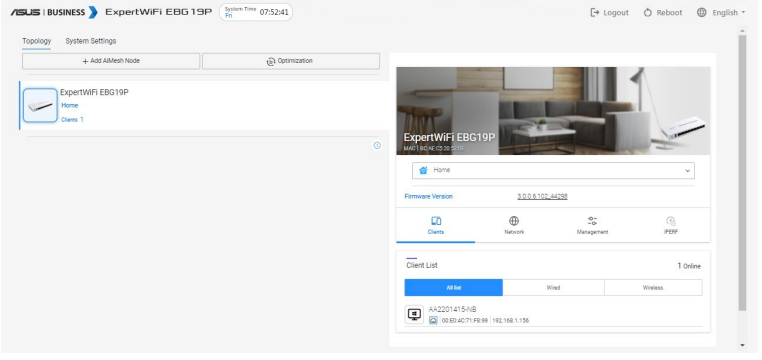
3.3 AiMesh

3.3.1 Configurar o sistema ExpertWiFi AiMesh

Para construir o seu sistema ExpertWiFi AiMesh, terá de configurar as suas definições.

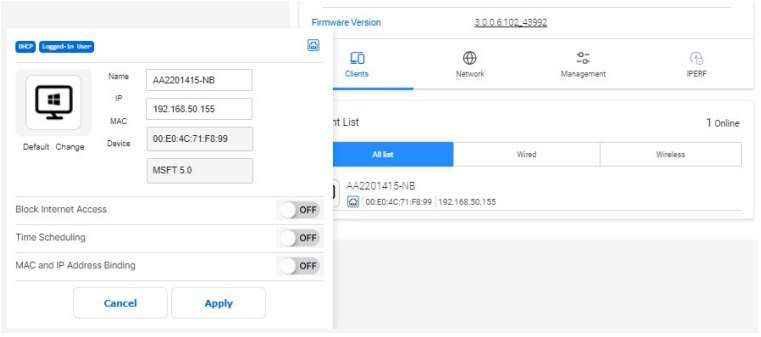
Para configurar as definições do sistema ExpertWiFi AiMesh:

1. No painel de navegação, aceda a **AiMesh** > **Topology (Topologia)**.
2. Pode clicar na parte inferior de **Set up as AiMesh Node (Configurar como nó AiMesh)** para adicionar os dispositivos ExpertWiFi sob o controlo do EBG19P.



3. Aceda a **AiMesh** > **System Settings (Definições do sistema)** para ativar ou desativar o **AiMesh node Ethernet auto setup (Configuração automática da Ethernet do nó AiMesh)**, **Ethernet Backhaul Mode (Modo Ethernet Backhaul)**, configurar a **Roaming Block List (Lista de bloqueio de roaming)**, **System Reset to Factory Default (Reposição das predefinições do sistema)** ou **System Reset (Reposição do sistema)**.

3.3.2 Gerir os clientes da sua rede

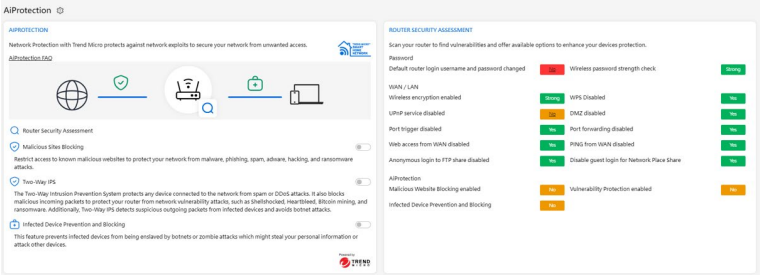


Para gerir os clientes da sua rede:

1. No painel de navegação, aceda a **AiMesh** > **Topology (Topologia)**.
2. Selecione o ícone **Clients (Clientes)** para visualizar as informações dos clientes da sua rede, tais como o nome do cliente, o endereço MAC e o endereço IP.
3. Pode bloquear o acesso do cliente à sua rede, desativar a sua programação horária ou desativar a vinculação de MAC e IP movendo o cursor para **OFF (DESATIVADO)**.
4. Clique em **Apply (Aplicar)** quando terminar.

3.4 AiProtection

O AiProtection oferece monotorização em tempo real que detecta malware, spyware e acessos não autorizados. Também filtra Web sites e aplicações não desejados e permite-lhe agendar quando um dispositivo ligado pode aceder à Internet.

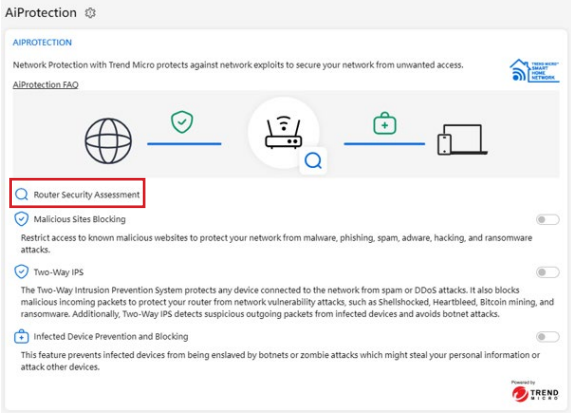


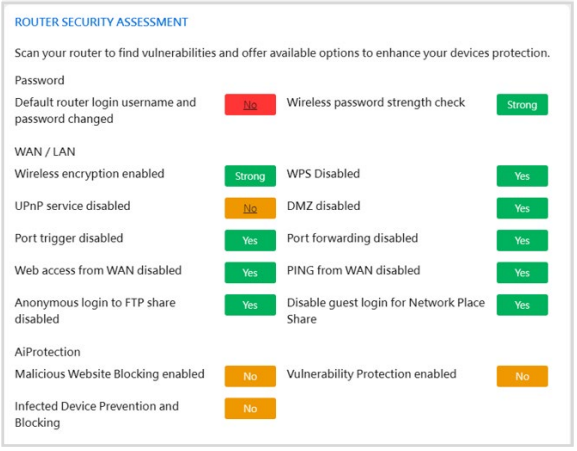
3.4.1 Protecção de rede

A Protecção de rede impede falhas de segurança de rede e protege-a contra acessos não autorizados.

Para avaliar a segurança do router:

1. No painel de navegação, aceda a **AiProtection**.
2. Clique em **Router Security Assessment (Avaliação de segurança do router)** para apresentar os resultados da avaliação de segurança.





IMPORTANTE! Os itens assinalados como **Yes (Sim)** na página **ROUTER SECURITY ASSESSMENT (AVALIAÇÃO DE SEGURANÇA DO ROUTER)** são considerados como safe (seguros). Quanto aos itens assinalados como **No (Não),** recomendamos que os configure correctamente.

3. (Opcional) Na página **ROUTER SECURITY ASSESSMENT (AVALIAÇÃO DE SEGURANÇA DO ROUTER)**, configure manualmente os itens assinalados como **No (Não)**. Para tal:

   a. Clique num item.

NOTA: Quando clicar num item, o utilitário encaminha-o para a página de configuração do mesmo.

   b. Na página de configuração de segurança do item, configure e efectue as alterações necessárias e clique em **Apply (Aplicar)** quando terminar.

   c. Volte à página **ROUTER SECURITY ASSESSMENT (AVALIAÇÃO DE SEGURANÇA DO ROUTER)** e clique em **Close (Fechar)** para sair da página.

4. Para configurar automaticamente as definições de segurança, clique em **Secure Your Router (Proteger o seu router).**

5. Quando for apresentado uma mensagem de aviso, clique em **OK**.

Para ativar a proteção da rede:

1. No painel de navegação, aceda a **AiProtection**.
2. Selecione o tipo de proteção que pretende implementar e deslize o seletor para o ativar. Pode escolher entre **Malicious Sites Blocking (Bloqueio de sites maliciosos)**, **Two-Way IPS (SPI bidirecional)** e **Infected Device Prevention and Blocking (Prevenção e bloqueio de dispositivos infetados)**.

   #### Bloqueio de sites maliciosos

   Esta funcionalidade restringe o acesso a sites maliciosos conhecidos para proteger a sua rede contra ataques de malware, phishing, spam, adware, hacking e ransomware.

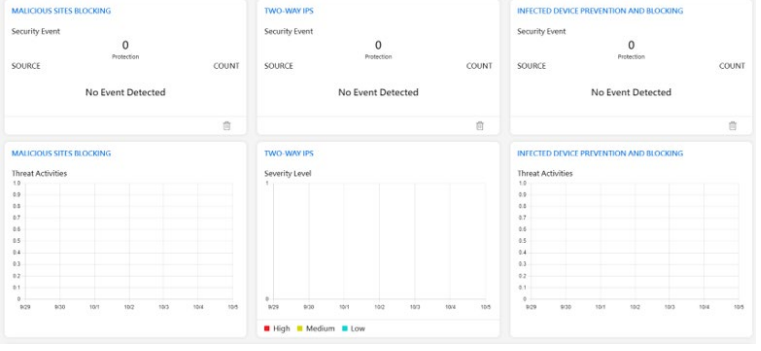
   #### IPS bidirecional

   O SPI (Sistema de Prevenção de Intrusões) bidirecional protege os dispositivos ligados contra ataques de spam ou DDoS. Também bloqueia a receção de pacotes maliciosos para proteger o seu router contra ataques de vulnerabilidade de rede, tais como Shellshocked, Heartbleed, mineração de Bitcoin e ransomware. Além disso, o SPI bidirecional deteta a saída de pacotes suspeitos de dispositivos infetados e evita ataques de botnet.

   #### Prevenção e bloqueio de dispositivos infectados

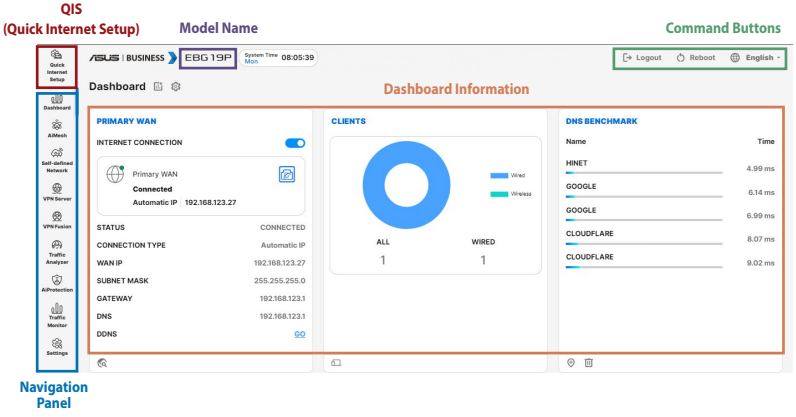
   Esta funcionalidade impede que os dispositivos infetados fiquem capturados devido a ataques de botnets ou zombies que podem roubar as suas informações pessoais ou atacar outros dispositivos.

3. Aceite o **Trend Micro End User License Agreement (Acordo de Licença do Utilizador Final da Trend Micro)**.



3.5 Painel de controlo

O painel de controlo permite-lhe gerir a sua rede, como a ligação à Internet, a ligação dos clientes, a referência DNS, o estado do sistema, a porta Ethernet e o monitor de tráfego.



3.6 Controlo de acesso de dispositivos

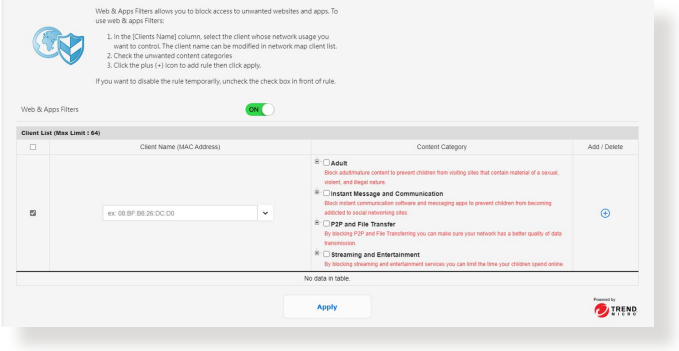
3.6.1 Filtros Web e de aplicações

Os Filtros de web e aplicações permitem bloquear o acesso a sites e aplicações indesejados.

Para utilizar os Filtros de web e aplicações:

1. No painel de navegação, aceda a **Settings (Definições)** > **Device access control (Controlo de acesso de dispositivos)** > **Web & Apps Filters (Filtros Web e de aplicações)**.
2. Deslize a barra para **ON (ATIVADO)** para ativar os **Web & Apps Filters (Filtros Web e de aplicações)**.
3. Na coluna **Client Name (Nome do cliente)**, selecione o cliente cuja utilização da rede deseja controlar. O nome do cliente pode ser modificado na lista de clientes do mapa de rede.
4. Marque as categorias de conteúdos não pretendidos.
5. Clique em ⊕ para adicionar uma regra e clique em **Apply (Aplicar)**.

Se pretender desativar temporariamente uma regra, desmarque a regra.

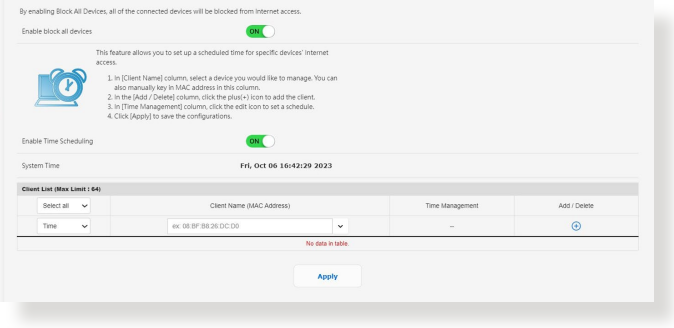


3.6.2 Agendamento

A programação horária permite definir uma hora programada para o acesso de dispositivos específicos à Internet.

Para utilizar a programação horária:

1. No painel de navegação, aceda a **Settings (Definições)** > **Device access control (Controlo de acesso de dispositivos)** > **Time Scheduling (Agendamento)**.
2. Deslize a barra para **ON (ATIVADO)** para ativar os **Enable Time Scheduling (Activar agendamento)**.
3. Na coluna **Client Name (Nome do cliente)**, seleccione ou introduza o nome do cliente a partir da caixa de lista pendente.
4. Clique em ⊕ para adicionar o perfil do cliente.
5. Clique em **Apply (Aplicar)** para guardar as definições.



3.7 Firewall

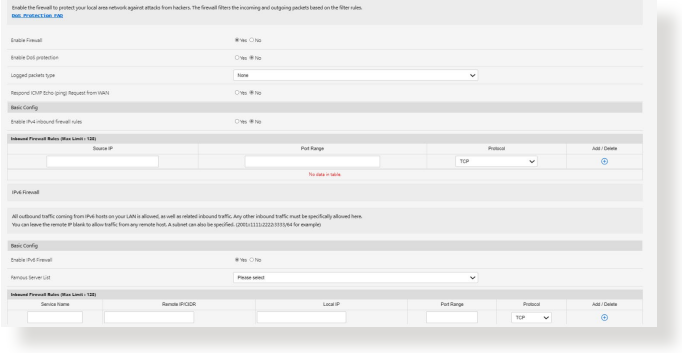
3.7.1 Geral

O router com fios pode funcionar como firewall de hardware para a sua rede.

NOTA: Esta funcionalidade de firewall está ativada por predefinição.

Para configurar as definições básicas da firewall:

1. No painel de navegação, aceda a **Settings (Definições)** > **Firewall** > **General (Geral)**.
2. No campo **Enable Firewall (Ativar firewall)**, selecione **Yes (Sim).**
3. No campo **Enable DoS (Ativar DoS)** protecção, selecione **Yes (Sim)** para proteger a sua rede contra ataques de DoS (Denial of Service), no entanto, isso poderá afectar o desempenho do router.
4. Pode também monitorizar pacotes transferidos entre a ligação LAN e WAN. No campo Logged packets type (Tipo de pacotes registados), Selecione **Dropped (Rejeitados)**, **Accepted (Aceites)** ou **Both (Ambos)**.
5. Clique em **Apply (Aplicar)**.



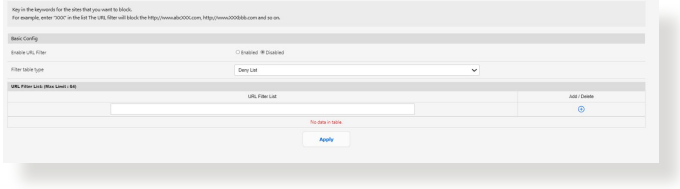
3.7.2 Filtro de URL

Pode especificar palavras-chave ou endereços Web para impedir o acesso a URLs específicos.

NOTA: O Filtro de URL é baseado numa consulta de DNS. Caso um cliente da rede tenha já acedido a um Web site como, por exemplo, http://www.abcxxx.com, esse Web site não será bloqueado (a cache de DNS do sistema armazena Web sites visitados anteriormente). Para resolver esse problema, limpe a cache de DNS antes de configurar o Filtro de URL.

Para configurar um filtro de URL:

1. No painel de navegação, aceda a **Settings (Definições)** > **Firewall** > **URL Filter (Filtro de URL)**.
2. No campo **Enable URL Filter (Ativar filtro de URL)**, selecione **Enabled (Ativado)**.
3. Introduza um URL e clique no botão ⊕.
4. Clique em **Apply (Aplicar)**.



3.7.3 Filtro de palavra-chave

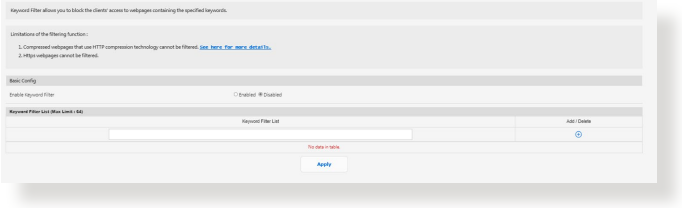
O filtro de palavra-chave bloqueia o acesso a páginas Web que contenham as palavras-chave especificadas.

Para configurar um filtro de palavra-chave:

1. No painel de navegação, aceda a **Settings (Definições)** > **Firewall** > **Keyword Filter (Filtro de palavra-chave)**.
2. No campo **Enable Keyword Filter (Ativar filtro de palavra-chave)**, selecione **Enabled (Ativado)**.
3. Introduza uma palavra ou frase e clique no botão ⊕.
4. Clique em **Apply (Aplicar)**.

NOTAS:

- O Filtro de palavra-chave é baseado numa consulta de DNS. Caso um cliente da rede tenha já acedido a um Web site como, por exemplo, http://www.abcxxx.com, esse Web site não será bloqueado (a cache de DNS do sistema armazena Web sites visitados anteriormente). Para resolver esse problema, limpe a cache de DNS antes de configurar o Filtro de palavra-chave.
- Não é possível filtrar páginas Web comprimidas utilizando a compressão HTTP. Também não é possível bloquear páginas HTTPS utilizando o filtro de palavra-chave.

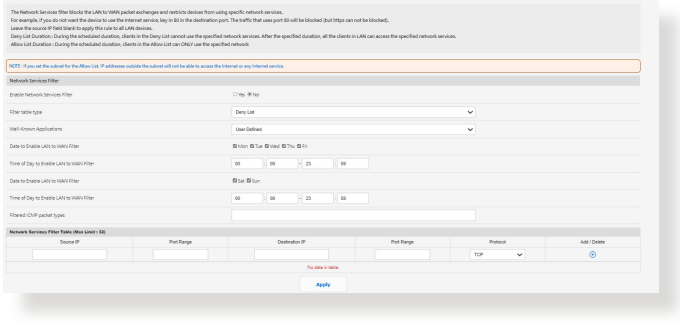


3.7.4 Filtro de Serviços de Rede

O Filtro de Serviços de Rede bloqueia transferências de pacotes da LAN para a WAN e impede que clientes da rede acedam a serviços Web específicos como, por exemplo, Telnet ou FTP.

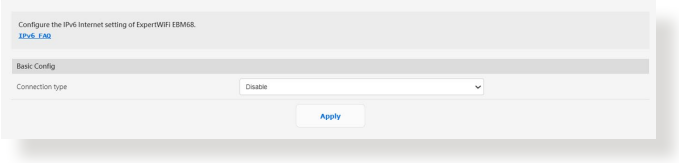
Para configurar um Filtro de Serviço de Rede:

1. No painel de navegação, aceda a **Settings (Definições)** > **Firewall** > **Network Service Filter (Filtro de Serviço de Rede)**.
2. No campo **Enable Network Services Filter (Ativar Filtro de Serviço de Rede)**, selecione **Yes (Sim)**.
3. Selecione o tipo de tabela de filtros. A **Deny List (Lista de recusas)** bloquei os serviços de rede especificados. A **Allow List (Lista de permissões)** limita o acesso apenas aos serviços de rede especificados.
4. Especifique o dia e a hora para Ativar os filtros.
5. Para especificar um Serviço de Rede a filtrar, introduza o IP de Origem, o IP de Destino, o Intervalo de Portas e o Protocolo. Clique no botão ⊕.
6. Clique em **Apply (Aplicar)**.



3.8 IPv6

Este router com fios suporta o endereçamento IPv6, um sistema que suporta mais endereços IP. Contacte o seu ISP para saber se o seu serviço de internet suporta IPv6.



Para configurar o IPv6:

1. No painel de navegação, aceda a **Settings (Definições)** > **IPv6**.
2. Selecione o seu **Connection Type (Tipo de ligação)**. As opções de configuração variam de acordo com o tipo de ligação selecionado.
3. Introduza as suas definições de LAN e DNS IPv6.
4. Clique em **Apply (Aplicar)**.

NOTAS:

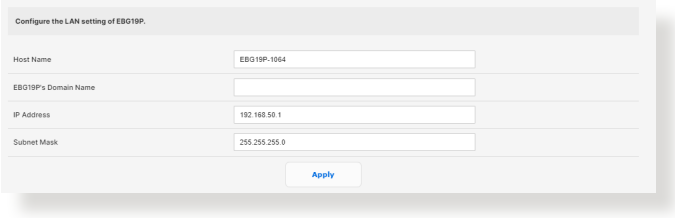
- Consulte o seu ISP para obter informações específicas sobre IPv6 para o seu serviço de Internet.
- Para mais informações, visite https://www.asus.com/support/FAQ/113990.

3.9 LAN

3.9.1 IP da LAN

O ecrã LAN IP (IP da LAN) permite-lhe modificar as definições de IP da LAN do seu router com fios.

NOTA: Quaisquer alterações ao endereço IP da LAN serão reflectidas nas definições de DHCP.

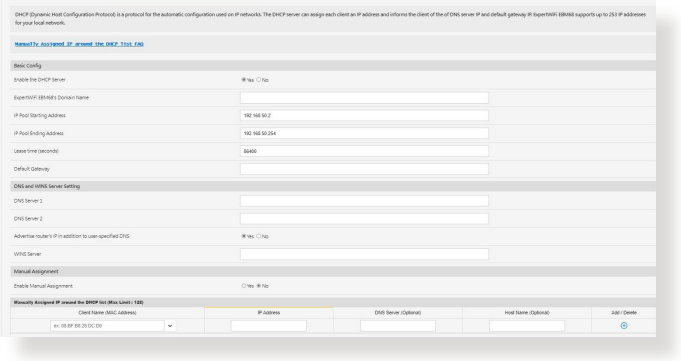


Para modificar as definições de IP da LAN:

1. No painel de navegação, aceda a **Settings (Definições)** > **LAN** > **LAN IP (IP da LAN)**.
2. Modifique os campos **IP address (Endereço IP)** e **Subnet Mask (Máscara de sub-rede)**.
3. Quando terminar, clique em **Apply (Aplicar)**.

3.9.2 DHCP Server

DHCP (Dynamic Host Configuration Protocol) é um protocolo para configuração automática utilizado em redes IP. O servidor DHCP pode atribuir um endereço IP a cada cliente e informar o cliente sobre o IP do servidor DNS e o IP do gateway predefinido.



Para configurar o servidor DHCP:

1. No painel de navegação, Clique em **Settings (Definições)** > **LAN** > **DHCP Server (Servidor DHCP)**.
2. No campo **Enable the DHCP Server (Ativar o servidor DHCP)**, marque **Yes (Sim)**.
3. Na caixa de texto **Domain Name (Nome de domínio)**, introduza um nome de domínio para o router com fios.
4. No campo **IP Pool Starting Address (Endereço inicial de conjunto de IP)**, introduza o endereço IP inicial.
5. No campo **IP Pool Ending Address (Endereço final de conjunto de IP)**, introduza o endereço IP final.
6. No campo **Lease Time (Tempo de concessão)**, introduza o tempo de validade dos endereços IP para que o router sem fios atribua automaticamente novos endereços IP para os clientes da rede.

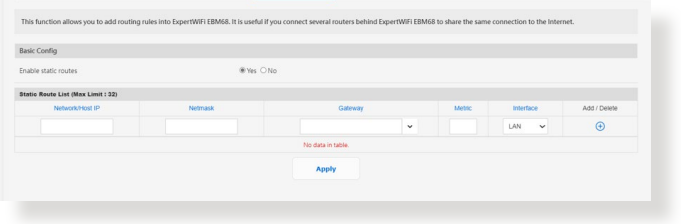
NOTAS:

- Recomendamos que utilize um endereço IP no formato 192.168.1.xxx (sendo que xxx pode ser qualquer número entre 2 e 254) quando especificar um intervalo de endereços IP.
- O endereço inicial do conjunto de IP não deverá ser superior ao endereço final do conjunto de IP.

7. Na secção **DNS and WINS Server Settings (Definições de DNS e WINS Servidor)**, Introduza o endereço IP do seu Servidor DNS e Servidor WINS, caso seja necessário.
8. O router com fios pode também atribuir manualmente os endereços IP aos dispositivos da rede. No campo **Enable Manual Assignment (Ativar atribuição manual)**, escolha **Yes (Sim)** para atribuir um endereço IP a endereços MAC específicos na rede. Podem ser adicionados até 32 endereços MAC à lista de DHCP para atribuição manual.

3.9.3 Encaminhamento

Esta função permite adicionar regras de encaminhamento para o router. É útil se ligar vários routers ao EBG19P para partilhar a mesma ligação à Internet.

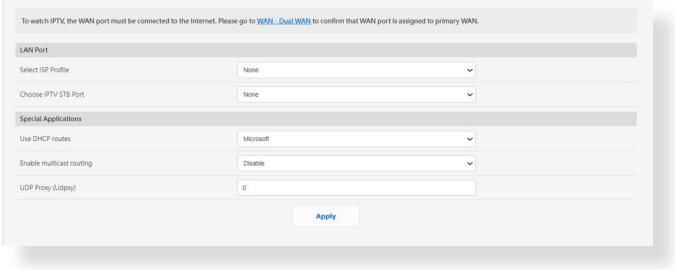


Para configurar a tabela de encaminhamento da LAN:

1. No painel de encaminhamento, aceda a **Settings (Definições)** > **LAN** > **Route (Encaminhamento)**.
2. No campo **Enable static routes (Ativar encaminhamentos estáticos)**, escolha **Yes (Sim)**.
3. Na secção **Static Route List (Lista de encaminhamento estático)**, introduza as informações de rede de outros pontos de acesso ou nós. Clique no botão ⊕ ou ⊖ para adicionar ou remover um dispositivo da lista.
4. Clique em **Apply (Aplicar)**.

3.9.4 IPTV

O router com fios suporta a ligação a serviços de IPTV através de um ISP ou uma LAN. O separador IPTV disponibiliza definições de configuração para IPTV, VoIP, multicasting e UDP para o seu serviço. Contacte o seu ISP para obter as informações específicas sobre o seu serviço.

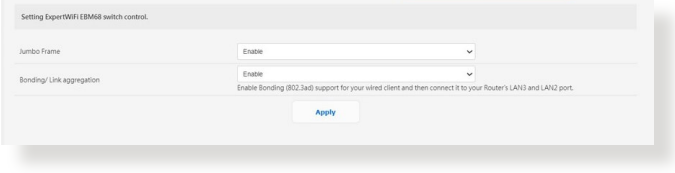


3.9.5 Controlo de comutação

Permite configurar o router para a função de controlo de comutação. Pode combinar duas portas LAN de 1 Gbps para disponibilizar velocidades com fio até 2 Gbps através da ligação ao seu NAS compatível ou a outro dispositivo de rede de largura de banda elevada.

NOTAS:

- Para utilizar a função Link Aggregation Control Protocol (LACP), os dispositivos devem suportar o protocolo IEEE 802.3ad.
- A função de agregação de LAN pode ser operada emparelhando a porta LAN3 com a porta LAN2.

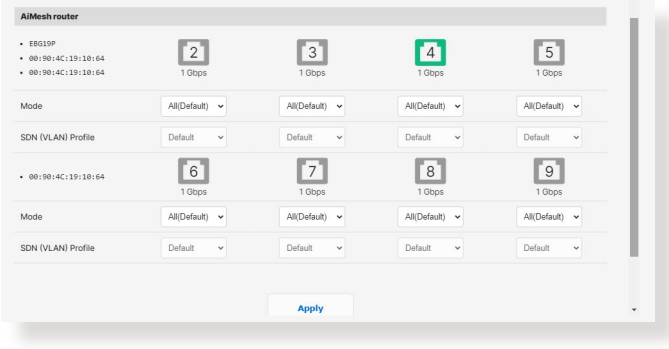


3.9.6 VLAN

Uma VLAN (Virtual Local Area Network) é uma rede lógica criada numa rede física maior. As VLAN permitem segmentar uma rede em sub-redes virtuais mais pequenas, que podem ser utilizadas para isolar o tráfego e melhorar o desempenho da rede.

Para configurar um VLAN:

1. No painel de encaminhamento, aceda a **Settings (Definições)** > **LAN** > **VLAN**.
2. Clique no separador **Profile (Perfil)** e, em seguida, clique em ⊕ para criar um perfil de VLAN. Pode atribuir a sua própria VLAN ID.
3. O **Port isolation (Isolamento de portas)** restringe o direito de acesso de diferentes dispositivos na mesma VLAN. Está a criar uma "Rede apenas VLAN", o que significa uma rede com VID mas sem DHCP.



4. Clique no separador **VLAN** para selecionar uma porta com um perfil e modo específico (**Trunk** / **Access**) (**Ramal / Acesso**).

NOTA: Pode selecionar um dos seguintes modos predefinidos:

All (Default) (Tudo (Predefinido)) permite o acesso a todos os pacotes marcados e não marcados.

O modo **Access (Acesso)** permite o acesso a uma SDN(VLAN) selecionada. É possível selecionar perfis criados pela rede de convidados ou por VLAN.

Modo **Trunk (Ramal)**:

- **Allow all tagged (Todos os identificados):** É permitido o acesso apenas a pacotes identificados.
- **With selected SDN (VLAN) (Com SDN (VLAN) selecionada):** É permitido o acesso apenas à SDN ou VLAN selecionada.

5. Clique em **Apply (Aplicar)** quando terminar.

NOTA: Para mais informações, visite https://www.asus.com/support/FAQ/1049415/.

3.10 Ferramentas de rede

Para utilizar as ferramentas de rede, no painel de navegação, aceda a **Settings (Definições)** > **Network Tools** (**Ferramentas de rede)**.

3.10.1 Análise de rede

Enviar pacotes ICMP ECHO_REQUEST aos anfitriões da rede.

3.10.2 Netstat

Exibir detalhes da rede.

3.10.3 Wake on LAN

A funcionalidade WOL (Wake-On-LAN) permite ativar um computador a partir de qualquer dispositivo na rede.

3.10.4 Regra de ligação inteligente

Configurar as informações relacionadas com Ligação inteligente.

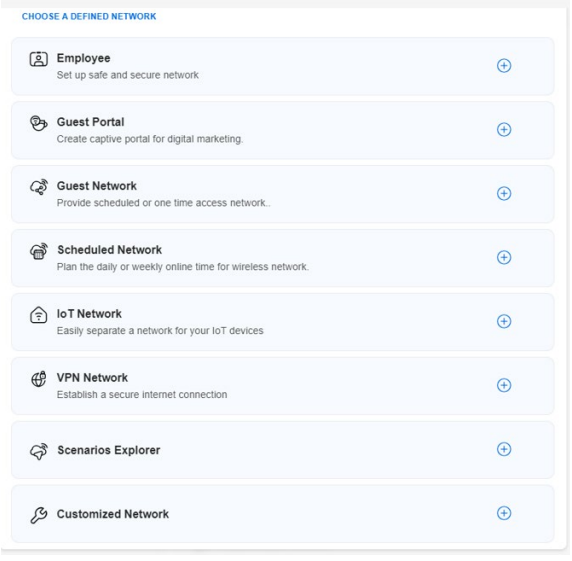
3.11 Rede autodefinida

Uma rede autodefinida (SDN) fornece até cinco SSID para separar e dar prioridade a dispositivos para diferentes utilizações comerciais e alternativas da rede, criando segmentos de rede para funcionários, portais de convidados, redes de convidados, redes programadas, redes IoT e redes VPN.

IMPORTANTE! Para tornar a função Wi-Fi disponível, integre um ponto de acesso (PA) sem fios, como ExpertWiFi EBA63 ou router, como ExpertWiFi EBR63 ou ExpertWiFi EBM68, na rede AiMesh do EBG19P.

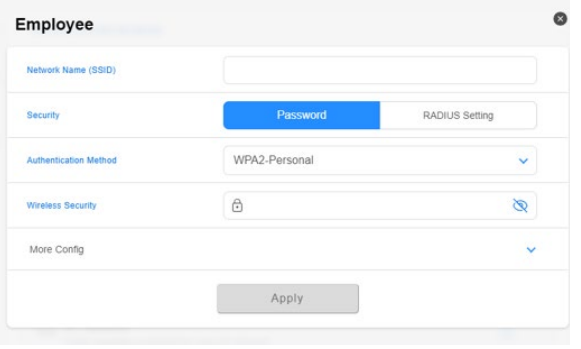
Para criar uma rede autodefinida:

1. No painel de navegação, aceda a **Self-Defined Network (Rede autodefinida)**.
2. Escolha uma rede definida que se adequa ao seu cenário específico.



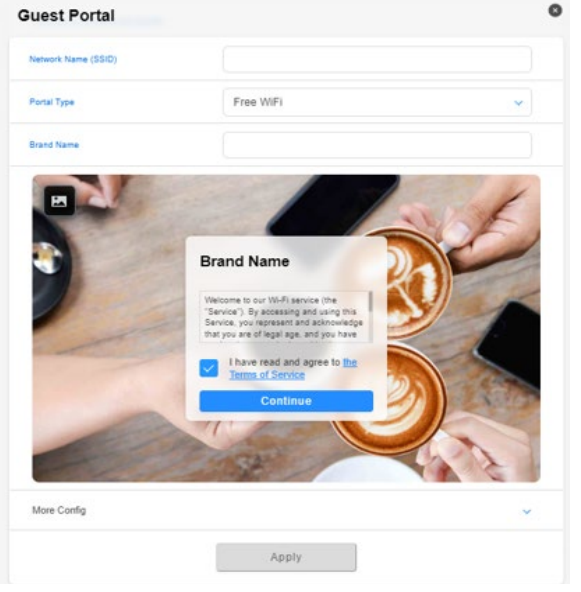
3.11.1 Funcionário

Permite definir o nível de acesso para diferentes utilizações, de modo a aumentar a segurança da rede. Recomendado para empresas que atribuem permissões a diferentes departamentos.



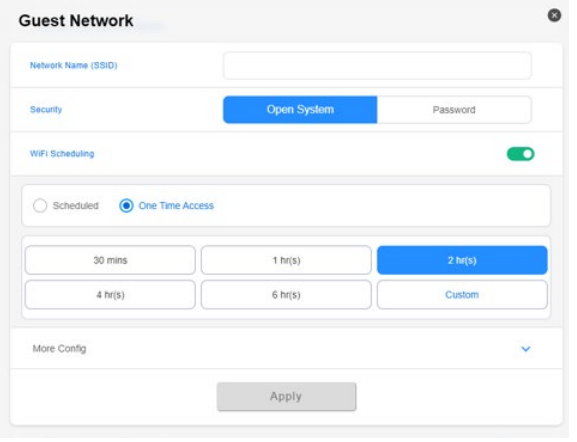
3.11.2 Portal de convidados

Permite criar um portal de convidados para marketing digital. Recomendado para utilização em restaurantes, hotéis ou camiões de transporte de produtos alimentares.



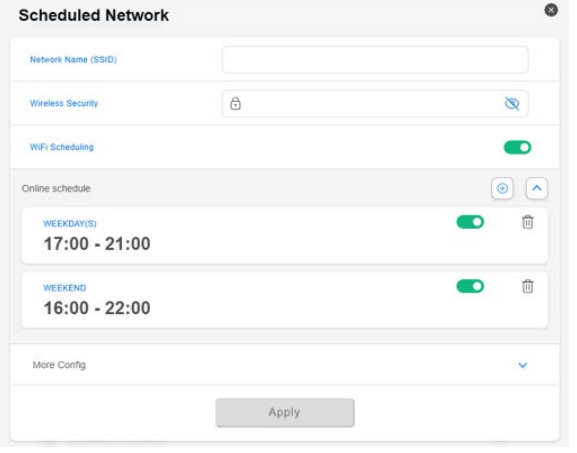
3.11.3 Rede de convidados

Fornece aos visitantes temporários um acesso programado ou único à rede. Recomendado para utilização em centros comerciais, ginásios ou para visitantes.



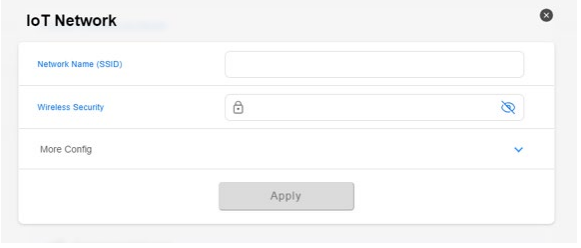
3.11.4 Rede programada

Planeia o tempo online diário ou semanal para a rede sem fios. Recomendado para ensino à distância, sala de aula ou uso infantil.



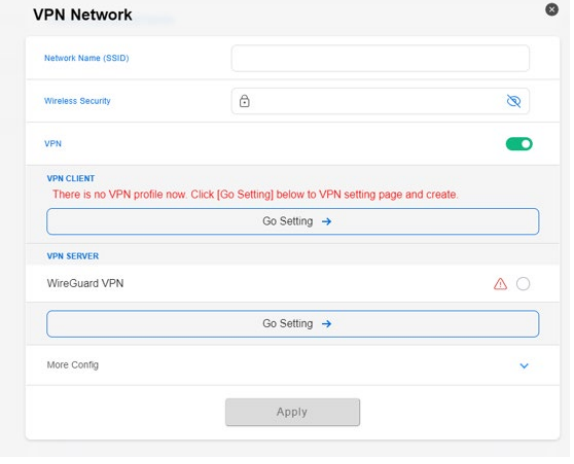
3.11.5 Rede IoT

Permite configurar facilmente uma rede separada para dispositivos IoT. Recomendado para utilização com dispositivos de vigilância, assistentes de voz, iluminação, câmaras de campainha, fechaduras inteligentes e sensores.



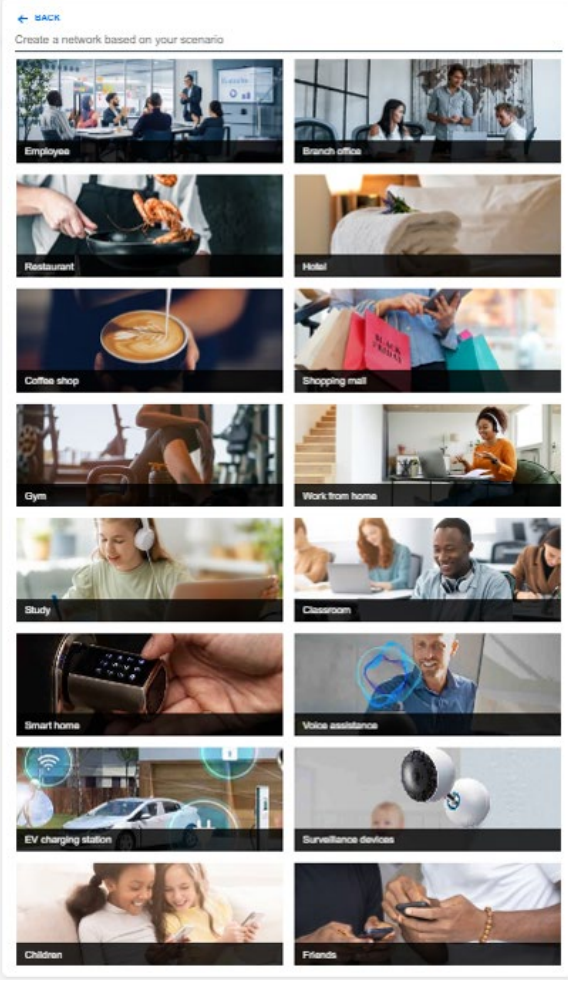
3.11.6 Rede VPN

Ajuda a estabelecer uma ligação segura à Internet através de VPN.



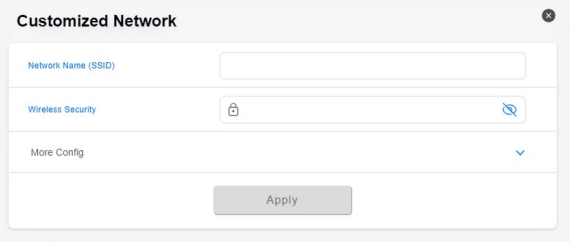
3.11.7 Explorador de cenários

Se não souber que rede criar, pode escolher o sector que corresponde à sua filiação para criar a rede.



3.11.8 Rede personalizada

Permite selecionar a opção de uma rede personalizada.



3.12 Registo do sistema

O registo do sistema contém o registo das actividades da sua rede.

NOTA: O registo do sistema será reposto quando o router for reiniciado ou desligado.

Para ver o registo do sistema:

1. No painel de navegação, aceda a **Settings (Definições)** > **System Log (Registo do sistema)**.

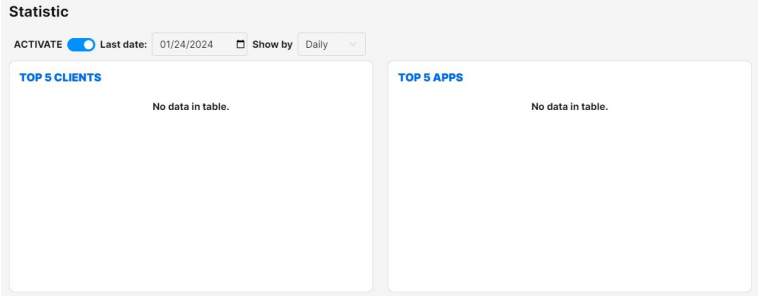
2. Pode ver as atividades da sua rede em quaisquer dos seguintes separadores:
   - Registo geral
   - Concessões DHCP
   - Reencaminhamento de portas
   - Tabela de encaminhamento
   - IPv6
   - Ligações

3.13 Monitor de tráfego

3.13.1 Analisador de Tráfego

Para utilizar o analisador de tráfego:

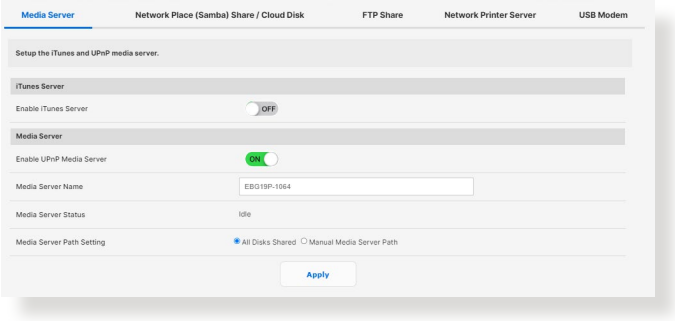
1. Ative a função **ACTIVATE (ATIVAR)**.
2. Atribua a última data a mostrar, e opte por monitorizar o tráfego de rede numa base diária, semanal ou mensal através de **Show by (Mostrar)** na lista pendente.
3. Serão exibidos os cinco melhores clientes, as cinco melhores aplicações, os dispositivos, o estado do cliente e a análise de aplicações.



3.14 Aplicação USB

3.14.1 Servidor Multimédia

O servidor multimédia permite configurar o servidor iTunes e UPnP.



Para abrir a página de configuração do Servidor Multimédia, aceda a **Settings (Definições)** > **USB Application (Aplicação USB)** > **Media Server (Servidor Multimédia)**.

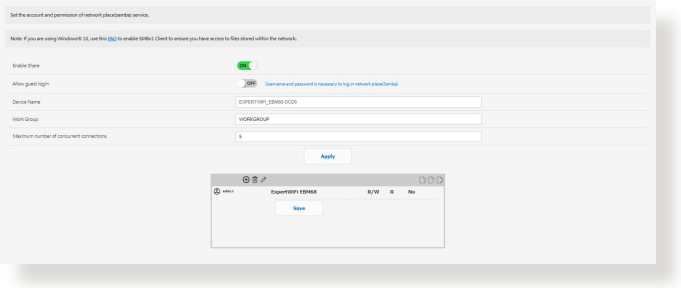
Consulte em seguida as descrições dos campos:

- **Ativar Servidor iTunes**: Selecione ON/OFF (ACTIVADO/ DESACTIVADO) para Ativar/desAtivar o Servidor iTunes.
- **Ativar Servidor Multimédia UPnP**: Selecione ON/OFF (ATIVADO/DESATIVADO) para Ativar/DesAtivar o Servidor Multimédia UPnP.
- **Nome do servidor de multimédia**: Introduza o nome do servidor de multimédia.
- **Definição do caminho do servidor multimédia:** Seleccione **All Disks Shared (Todos os discos partilhados)** ou **Manual Media Server Path (Caminho do servidor multimédia manual).**

Clique em **Apply (Aplicar)** quando terminar.

3.14.2 Partilha de local de rede (Samba)

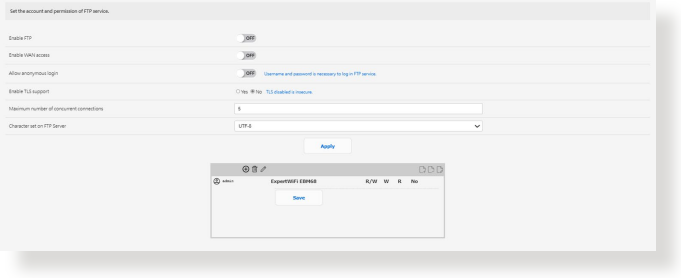
A Partilha de Local de Rede (Samba) permite configurar a conta e permissões para o serviço samba.



Para utilizar a Partilha Samba, aceda a **Settings (Definições)** > **USB Application (Aplicação USB)** > **Network Place (Samba) Share (Partilha de local de rede (Samba))**.

3.14.3 Partilha FTP

A Partilha FTP permite configurar as contas e permissões para o serviço FTP.



Para utilizar a Partilha FTP, aceda a **Settings (Definições)** > **USB Application (Aplicação USB)** > **FTP Share (Partilha FTP)**.

3.14.4 Servidor de impressora de rede

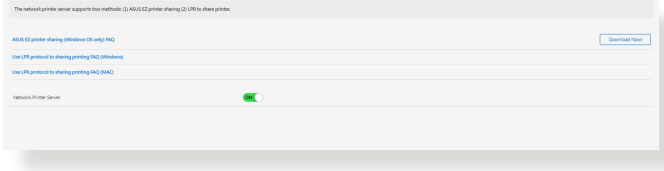
3.14.4.1 ASUS EZ Printer Sharing

O utilitário ASUS EZ Printing Sharing permite-lhe ligar uma impressora USB à porta USB do seu router com fios e configurar o servidor de impressão Isso permite que os clientes da sua rede imprimam e digitalizem ficheiros através da ligação sem fios.

NOTA: A função de servidor de impressão é suportada no Windows® 10 e Windows® 11.

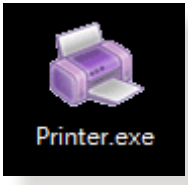
Para configurar o modo de partilha do EZ Printer:

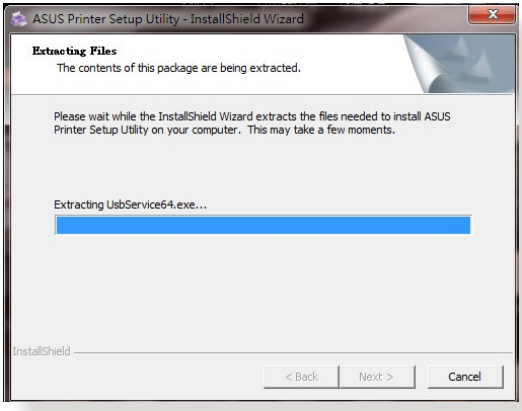
1. No painel de navegação, aceda a **Settings (Definições)** > **USB Application (Aplicação USB)** > **Network Printer Server**.
2. Clique em **Download Now! (Transferir agora!)** para transferir o utilitário de impressora de rede.



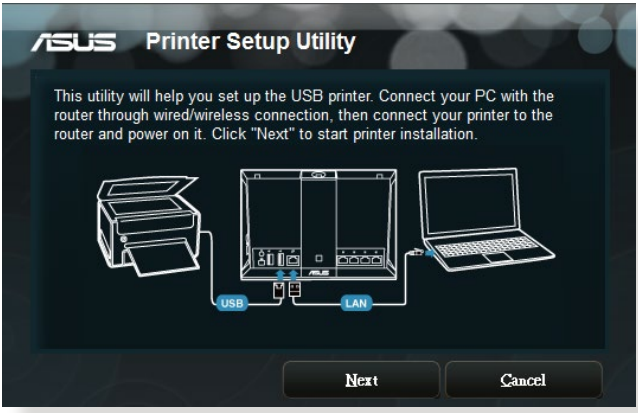
NOTA: O utilitário de impressora de rede é suportado apenas no Windows® 10 e Windows® 11. Para instalar o utilitário no Mac OS, Selecione **Use LPR protocol for sharing printer (Utilizar protocolo LPR para partilhar impressora)**.

3. Descomprima o ficheiro transferido e clique no ícone da Impressora para executar o programa de configuração da impressora de rede.



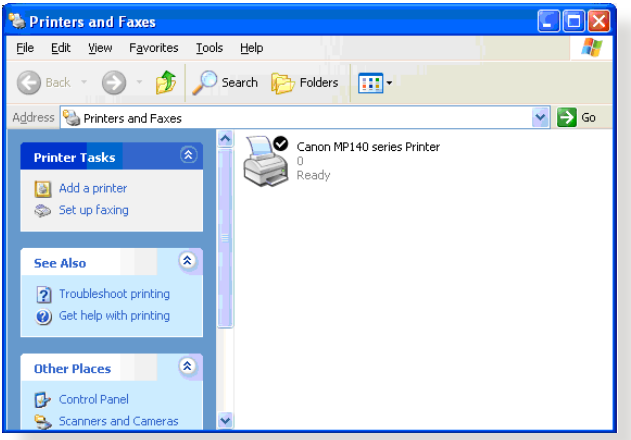


4. Siga as instruções para configurar o hardware e depois clique em **Next (Seguinte)**.



5. Aguarde alguns minutos pela conclusão da configuração inicial. Clique em **Next (Seguinte)**.
6. Clique em **Finish (Concluir)** para concluir a instalação.
7. Siga as instruções do sistema operativo Windows® para instalar o controlador da impressora.

8. Após a instalação do controlador da impressora, os clientes da rede poderão utilizar a impressora.

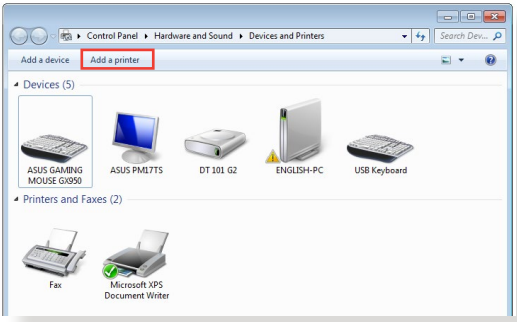


3.14.4.2 Utilizar LPR para partilhar a impressora

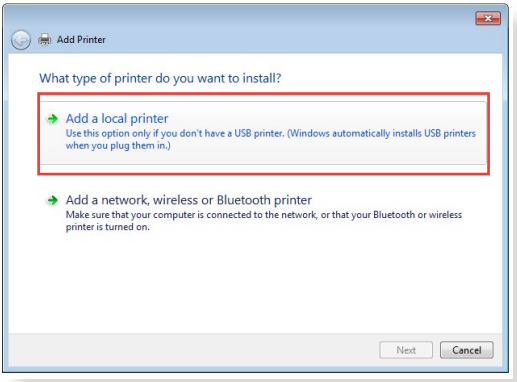
Pode partilhar a sua impressora com computadores com os sistemas operativos Windows® e MAC utilizando LPR/LPD (Line Printer Remote/Line Printer Daemon).

Para partilhar a sua impressora LPR:

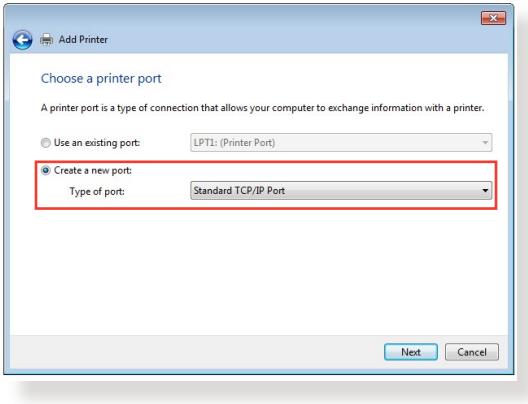
1. No ambiente de trabalho do Windows®, clique em **Start (Iniciar)** > **Devices and Printers (Dispositivos e Impressoras)** > **Add a printer (Adicionar uma impressora)** para executar o **Add Printer Wizard (Assistente para Adicionar Impressoras)**.



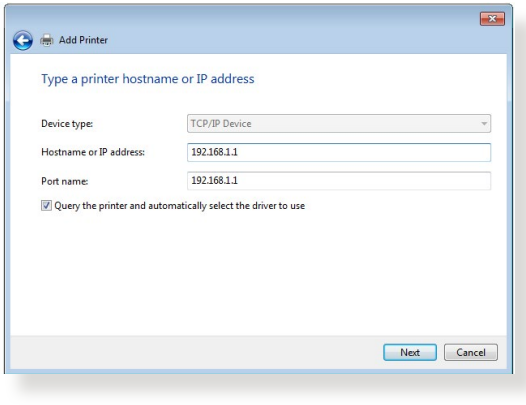
2. Selecione **Add a local printer (Adicionar uma impressora local)** e clique em **Next (Seguinte)**.



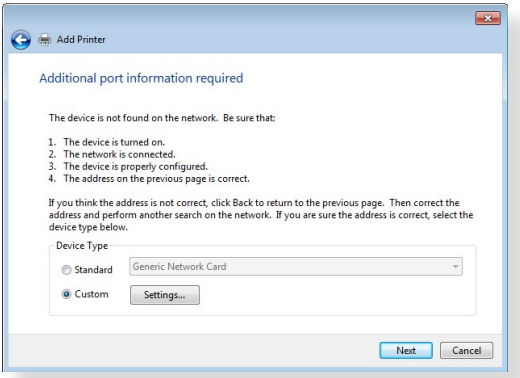
3. Selecione **Create a new port (Criar uma nova porta)** e defina o **Type of Port (Tipo de porta)** como **Standard TCP/IP Port (Porta TCP/IP Padrão)**. Clique em **New Port (Nova porta)**.



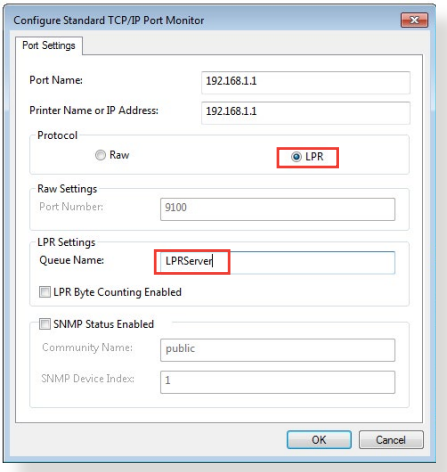
4. No campo **Hostname or IP address (Nome do anfitrião ou endereço IP)**, introduza o endereço IP do router com fios e clique em **Next (Seguinte)**.



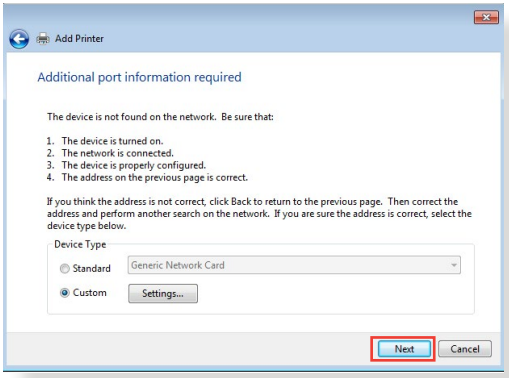
5. Selecione **Custom (Personalizado)** e clique em **Settings (Definições)**.



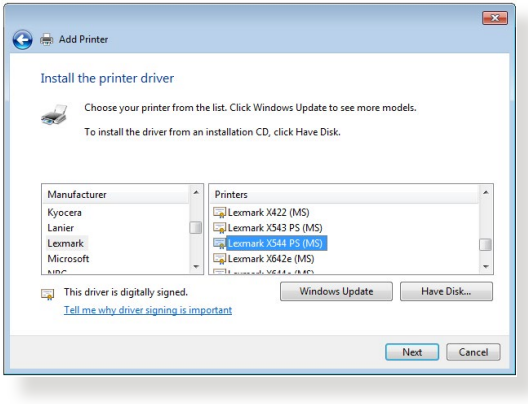
6. Defina o **Protocol (Protocolo)** como **LPR**. No campo **Queue Name (Nome da fila)**, introduza o **LPRServer (Servidor LPR)** e clique em **OK** para continuar.



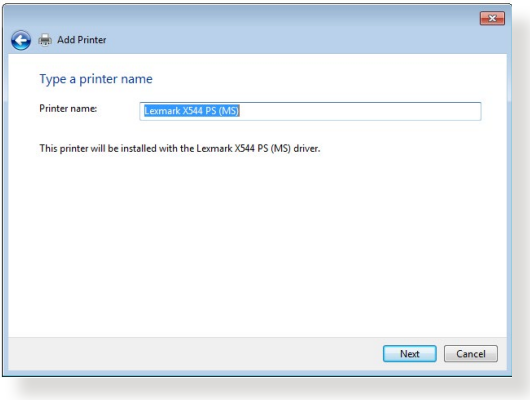
7. Clique em **Next (Seguinte)** para concluir a configuração da porta TCP/IP padrão.



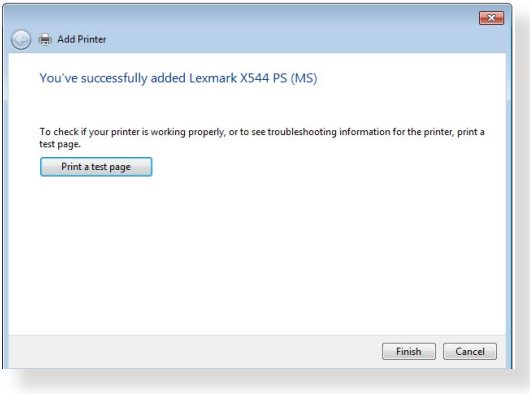
8. Instale o controlador da impressora a partir da lista de fabricantes-modelos. Se a impressora não constar da lista, clique em **Have Disk (Disco)** para instalar manualmente os controladores da impressora a partir de um CD-ROM ou ficheiro.



9. Clique em **Next (Seguinte)** para aceitar o nome predefinido para a impressora.



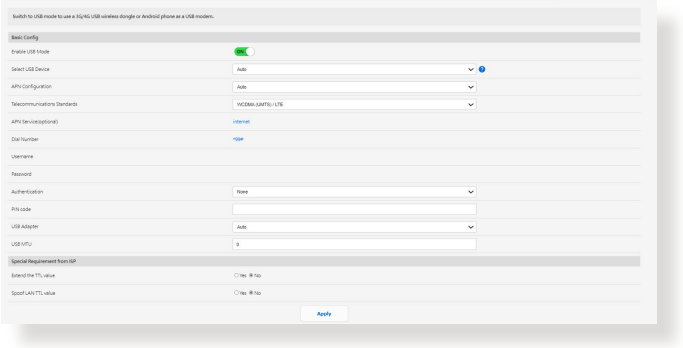
10. Clique em **Finish (Concluir)** para concluir a instalação.



3.14.5 Modem USB

Mudar para o modo USB para utilizar um adaptador sem fios USB 3G/4G ou um telemóvel Android como modem USB.

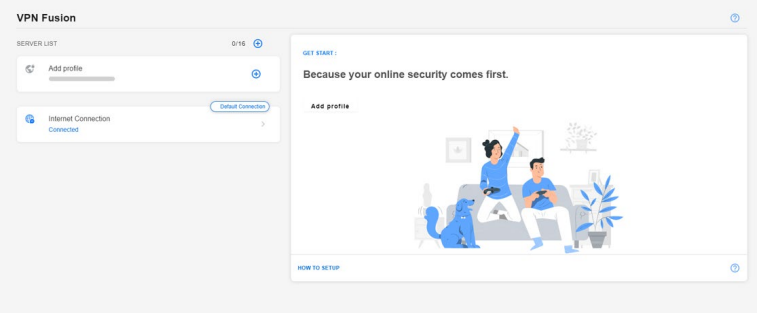
Para utilizar o modem USB, aceda a **Settings (Definições)** > **USB Application (Aplicação USB)** > **USB Modem (Modem USB)**.



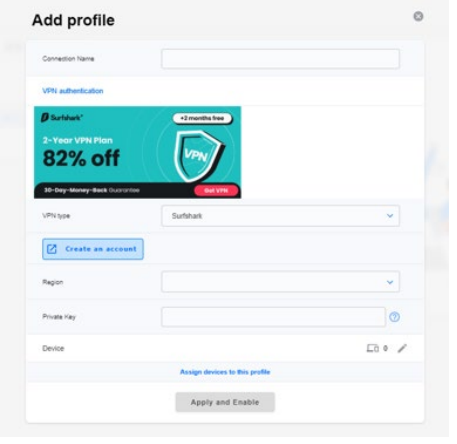
3.15 Fusão de VPN

3.15.1 Criar uma fusão de VPN

O VPN Fusion permite ligar a vários servidores VPN em simultâneo e definir dispositivos cliente para ligar a túneis VPN diferentes.

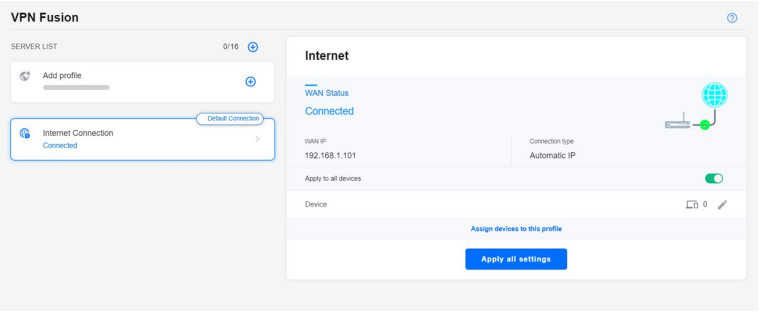


1. No painel de navegação, aceda a **VPN Fusion (Fusão de VPN)**.
2. Clique em ⊕ no campo **Add profile (Adicionar perfil)** para configurar um novo túnel VPN.
3. Conclua a configuração da VPN, incluindo o nome da ligação, o tipo de VPN, a região, a chave privada e o dispositivo.
4. Clique em **Apply and Enable (Aplicar e ativar)**.



3.15.2 Ligação à Internet

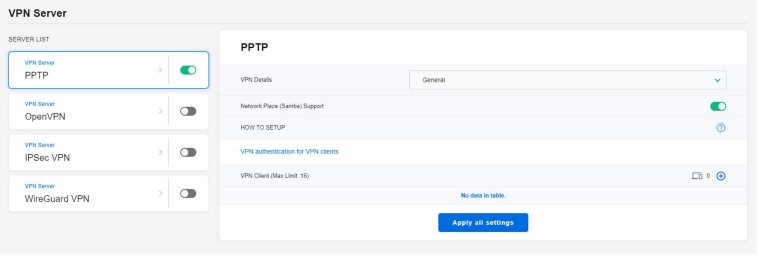
Permite gerir o estado da WAN dos dispositivos ligados.



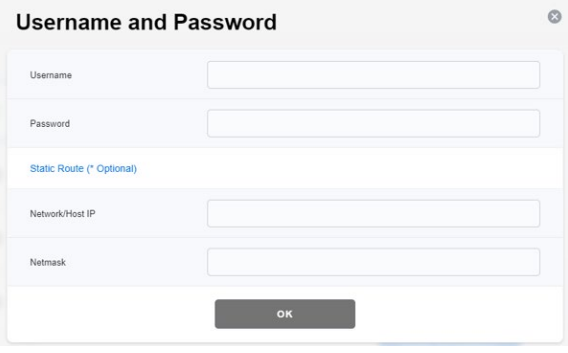
3.16 Servidor VPN

3.16.1 PPTP

1. No painel de navegação, aceda a **VPN Server (Servidor VPN)** > **PPTP** e desloque o cursor para a direita (por predefinição, está desativado no lado esquerdo).
2. No campo **VPN Client (Max Limit: 16) (Cliente VPN (Limite máx.: 16)**), clique em ⊕ para adicionar uma conta.



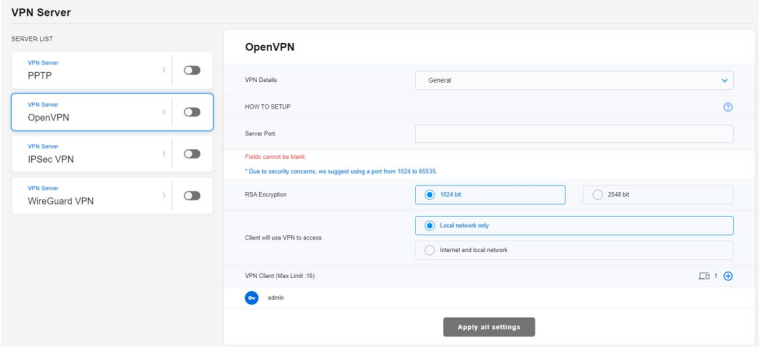
3. Introduza um *[Nome de utilizador]* e *[Palavra-passe]* personalizados, e clique em **OK**.



NOTA: Depois de definidos, o *[Nome de utilizador]* e a *[Palavra-passe]* não podem ser alterados. Para mais informações, visite https://www.asus.com/support/FAQ/114892/.

3.16.2 OpenVPN

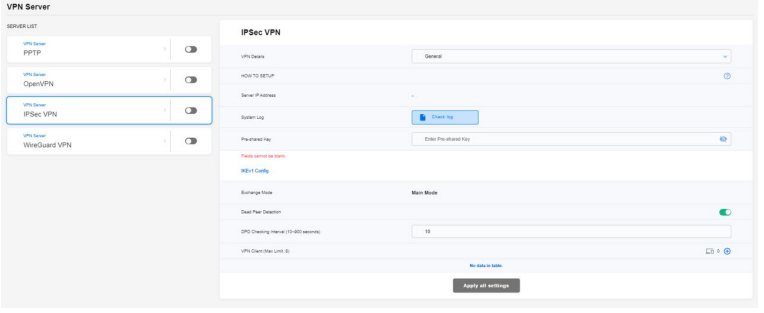
1. No painel de navegação, aceda a **VPN Server (Servidor VPN)** > **OpenVPN** e desloque o cursor para a direita (por predefinição, está desativado no lado esquerdo).
2. Configure as definições gerais no campo **VPN Details (Detalhes de VPN)**.
3. Introduza o seu nome de utilizador e a palavra-passe na coluna em branco.
4. No campo **VPN Client (Max Limit: 16) (Cliente VPN (Limite máx.: 16)**), clique em ⊕ para adicionar uma conta.
5. A palavra-passe é automaticamente oculta. Clique em **Apply all settings (Aplicar todas as definições)**.



NOTA: Para mais informações, visite https://www.asus.com/support/FAQ/1008713/.

3.16.3 IPSec VPN

1. No painel de navegação, aceda a **VPN Server (Servidor VPN)** > **IPSec VPN** e desloque o cursor para a direita (por predefinição, está desativado no lado esquerdo).
2. Introduza uma chave no campo **Pre-sahred Key (Chave pré-partilhada)**.
3. No campo **VPN Client (Max Limit: 8) (Cliente VPN (Limite máx.: 8)**), clique em ⊕ para adicionar uma conta.
4. Introduza um *[Nome de utilizador]* e *[Palavra-passe]* personalizados, e clique em **Apply all settings (Aplicar todas as definições)**.

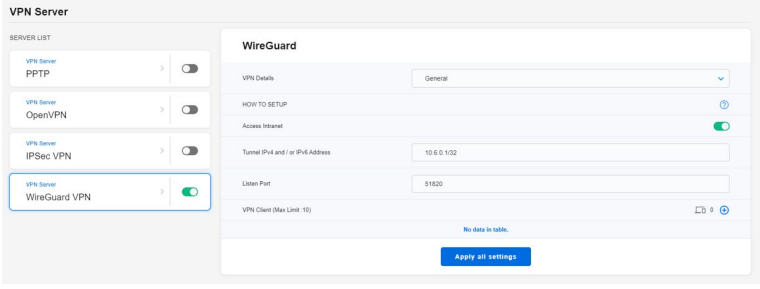


NOTA: Depois de definidos, o *[Nome de utilizador]* e a *[Palavra-passe]* não podem ser alterados. Para mais informações, visite https://www.asus.com/support/FAQ/1044190/.

3.16.4 VPN WireGuard®

1. No painel de navegação, aceda a **VPN Server (Servidor VPN)** > **WireGuard VPN (VPN WireGuard)**.
2. No campo **VPN Client (Max Limit: 10) (Cliente VPN (Limite máx.: 10)**), clique em ⊕ para adicionar uma conta. Para dispositivos gerais, como computadores portáteis ou smartphones, clique em **Apply (Aplicar).**
3. Clique em **Apply all settings (Aplicar todas as definições)** para ativar a VPN WireGuard®.
4. Clique em" ••• " para mais detalhes.

NOTA: Se estiver a utilizar um smartphone para se ligar à VPN WireGuard®, transfira a aplicação WireGuard® do Google Play ou da App Store e faça a leitura do código na aplicação para transferir o ficheiro de configuração.

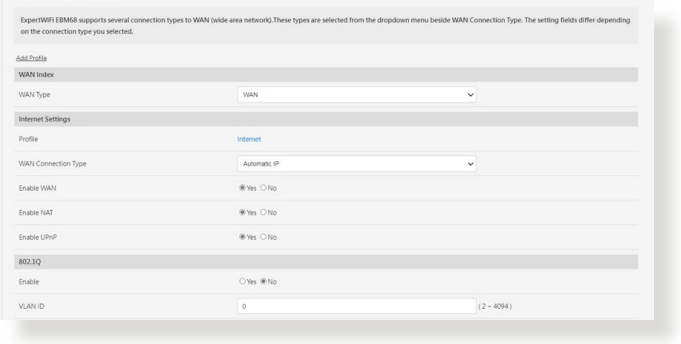


NOTA: Para mais informações, visite https://www.asus.com/support/FAQ/1048280/.

3.17 WAN

3.17.1 Ligação à Internet

O ecrã Internet Connection (Ligação à Internet) permite-lhe configurar as definições de vários tipos de ligação WAN.



Para configurar as definições de ligação WAN:

1. No painel de navegação, aceda a **Settings (Definições)** > **WAN** > **Internet Connection (Ligação à Internet)**.
2. Configure as definições indicadas abaixo. Quando terminar, clique em **Apply (Aplicar)**.

- **Tipo de ligação WAN**: Escolha o seu tipo de Fornecedor de Serviços de Internet. As escolhas são **Automatic IP (IP automático)**, **PPPoE**, **PPTP**, **L2TP** ou **Static IP (IP estático)**. Consulte o seu ISP se o router não conseguir obter um endereço IP válido ou se tem dúvidas acerca do tipo de ligação WAN.
- **Ativar WAN**: Seleccione **Yes (Sim)** para permitir que o router aceda à Internet. Selecione **No (Não)** para desativar o acesso à Internet.
- **Ativar NAT**: NAT (Network Address Translation) é um sistema em que um IP público (WAN IP) é utilizado para fornecer acesso à Internet a clientes da rede com um IP privado numa LAN. O endereço IP privado de cada cliente da rede será guardado numa tabela NAT e utilizado para encaminhar pacotes de dados recebidos.

- **Ativar UPnP**: UPnP (Universal Plug and Play) permite que diversos dispositivos (como, por exemplo, routers, televisores, sistemas de áudio, consolas de jogos e telemóveis), sejam controlados através de uma rede baseada em IP com ou sem controlo central através de um gateway. UPnP liga a todos os tipos de PCs, oferecendo uma rede contínua para configuração remota e transferência de dados. Através da função UPnP, os novos dispositivos de rede são descobertos automaticamente. Após a ligação à rede, os dispositivos podem ser configurados remotamente para suportar aplicações P2P, jogos interativos, videoconferência e servidores Web ou proxy. Ao contrário do reencaminhamento de portas, que envolve a configuração manual das definições das portas, a função UPnP configura automaticamente o router para aceitar ligações recebidas e pedidos diretos para um PC específico na rede local.
- **Ligar ao servidor DNS**: Permite que o router obtenha o endereço IP DNS automaticamente a partir do ISP. Um DNS é um anfitrião na Internet que converte nomes da Internet em endereços IP numéricos.
- **Autenticação**: Este item poderá ser especificado por alguns ISPs. Consulte o seu ISP e preencha os dados, caso seja necessário.
- **Nome do anfitrião**: Este campo permite-lhe atribuir um nome de anfitrião ao seu router. Este é geralmente um requisito especial do ISP. Se o seu ISP atribuiu um nome de anfitrião ao seu computador, introduza aqui o nome de anfitrião.
- **Endereço MAC**: O endereço MAC (Media Access Control) é um identificador exclusivo para o seu dispositivo de rede. Alguns ISPs monitorizam o endereço MAC dos dispositivos de rede que se ligam ao seu serviço e rejeitam quaisquer dispositivos não reconhecidos que tentem ligar. Para evitar problemas de ligação devido a endereços MAC não reconhecidos, pode:
  - Contactar o seu ISP e atualizar o endereço MAC associado ao serviço do seu ISP.
  - Efetuar a clonagem ou alteração do endereço MAC do router com fios ASUS para coincidir com o endereço MAC do dispositivo original reconhecido pelo ISP.

3.17.2 Multi-WAN

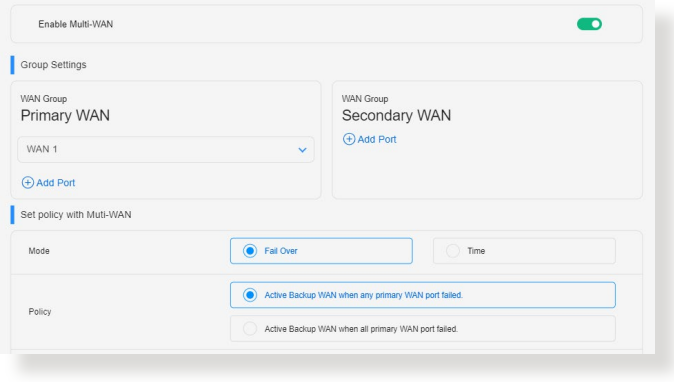
A opção Multi-WAN permite-lhe selecionar várias ligações ISP para o seu router e os grupos WAN para as WAN principal e secundária.

Para configurar a Multi-WAN:

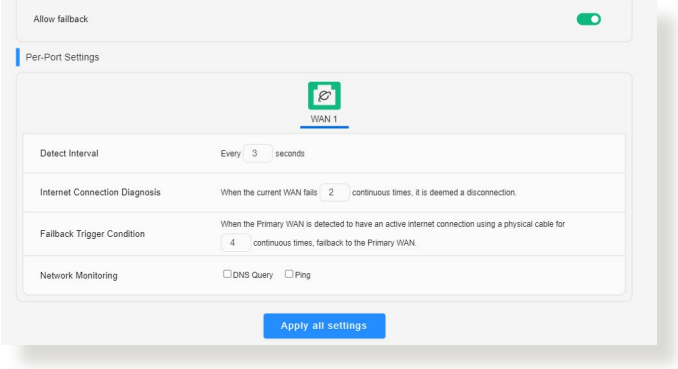
1. No painel de navegação, aceda a **Settings (Definições) > WAN > Multi-WAN**.
2. Ative a função **Enable Multi-WAN (Ativar Multi-WAN)**.
3. **Escolha a Primary WAN (WAN principal)** e **Secondary WAN (WAN secundária)**. As opções são: WAN, USB e Ethernet LAN.
4. Escolha **Fail Over (Ativação pós-falha)** ou **Time (Hora)**.

   Fail Over (Ativação pós-falha): Utilizar uma WAN secundária para acesso de reserva à rede.

   Time (Hora): Defina a hora para agendar a sua política Multi-WAN.
5. Escolha **Active Backup WAN when any primary WAN port failed (Ativar WAN de cópia de segurança quando qualquer porta WAN principal falhar)** ou **Active Backup WAN when all primary WAN port failed (Ativar WAN de cópia de segurança quando todas as portas WAN principais falharem)**.



6. Ative ou desative a opção **Allow failback (Permitir reativação)** pós-falha. .
7. Especifique o intervalo de deteção.
8. Especifique o número de tempos de falha contínuos antes de a WAN atual ser considerada desligada.
9. Especifique o número de vezes contínuas que a WAN principal é detetada como tendo uma ligação ativa à Internet através de um cabo físico, que aciona uma reativação pós-falha na WAN principal.
10. Escolha **DNS Query (Consulta DNS)** ou **Ping**.
11. Clique em **Apply all settings (Aplicar todas as definições)**.



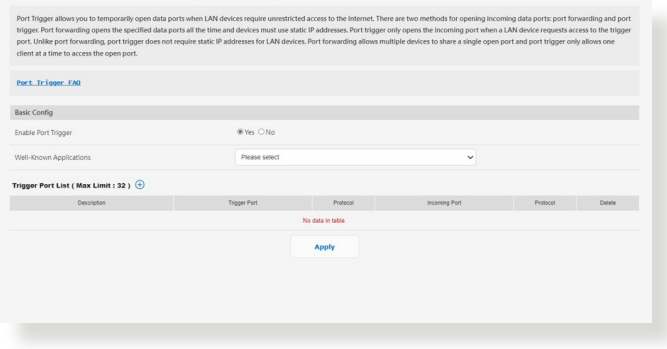
NOTA: Estão disponíveis explicações detalhadas na secção Perguntas frequentes do site de apoio da ASUS **https://www.asus.com/support/FAQ/1011719**.

3.17.3 Ativação de Portas

A Ativação de portas permite ativar temporariamente as portas de dados quando os dispositivos LAN necessitam de acesso ilimitado à Internet. Existem dois métodos para abrir portas de entrada de dados: o reencaminhamento de portas e a ativação de portas.

- O reencaminhamento de portas ativa sempre as portas de dados especificadas e os dispositivos devem utilizar endereços IP estáticos.
- A ativação de portas ativa a porta de entrada apenas quando um dispositivo LAN solicita acesso à porta ativada.

Ao contrário do reencaminhamento de portas, a ativação de portas não requer endereços IP estáticos para dispositivos da LAN. O reencaminhamento de portas permite que vários dispositivos partilhem uma única porta aberta e a ativação de portas permite apenas que um cliente de cada vez aceda à porta aberta.



Para configurar a Activação de Portas:

1. No painel de navegação, aceda a **Settings (Definições)** > **WAN** > **Port Trigger (Activação de Portas)**.
2. Configure as definições indicadas abaixo. Quando terminar, clique em **Apply (Aplicar)**.
   - **Ativar Ativação de Portas**: Escolha **Yes (Sim)** para Ativar a Ativação de Portas.
   - **Aplicações conhecidas**: Selecione jogos e serviços Web populares para adicionar à Lista de Ativação de Portas.

- **Descrição**: Introduza um nome abreviado ou uma descrição para o serviço.
- **Porta de ativação**: Especifique uma porta de activação para abrir a porta de entrada.
- **Protocolo**: Selecione o tipo de protocolo, TCP ou UDP.
- **Incoming Port (Porta de entrada)**: Especifique uma porta de entrada para receber dados da Internet.

NOTAS:

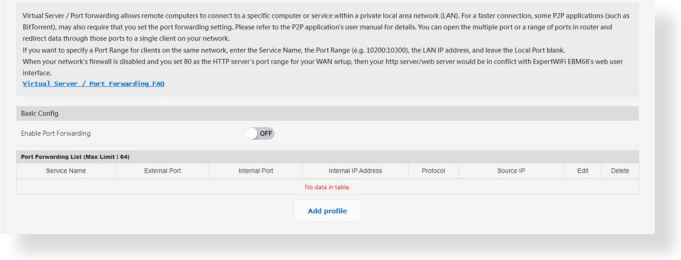
- Ao ligar-se a um servidor de IRC, um PC cliente efetua uma ligação de saída utilizando o intervalo de ativação de portas 66660-7000. O servidor de IRC responde verificando o nome de utilizador e criando uma nova ligação ao PC cliente através de uma porta de entrada.
- Se a Ativação de Portas estiver desativada, o router interrompe a ligação porque não é capaz de determinar qual o PC que está pedir acesso ao IRC. Quando a Ativação de Portas está ativada, o router atribui uma porta de entrada para receber os dados. Esta porta de entrada fecha quando terminar um período de tempo específico porque o router não sabe quando a aplicação foi terminada.
- A ativação de portas permite que um cliente da rede utilize apenas um determinado serviço e uma porta de entrada em simultâneo.
- Não é possível utilizar a mesma aplicação para ativar uma porta em mais do que um PC em simultâneo. O router irá reencaminhar apenas a porta para o último computador que enviar um pedido/ativação para o router.
- Para mais informações, visite https://www.asus.com/support/FAQ/114110.

3.17.4 Servidor virtual/Reencaminhamento de portas

Servidor virtual / reencaminhamento de portas permite que computadores remotos se liguem a um computador ou serviço específico numa rede local privada (LAN). Para uma ligação mais rápida, algumas aplicações P2P (como BitTorrent) podem também exigir a definição de reencaminhamento de portas. Para mais informações, consulte o manual do utilizador da aplicação P2P. Pode ativar várias portas ou um intervalo de portas no router e redirecionar os dados através dessas portas para um único cliente na sua rede.

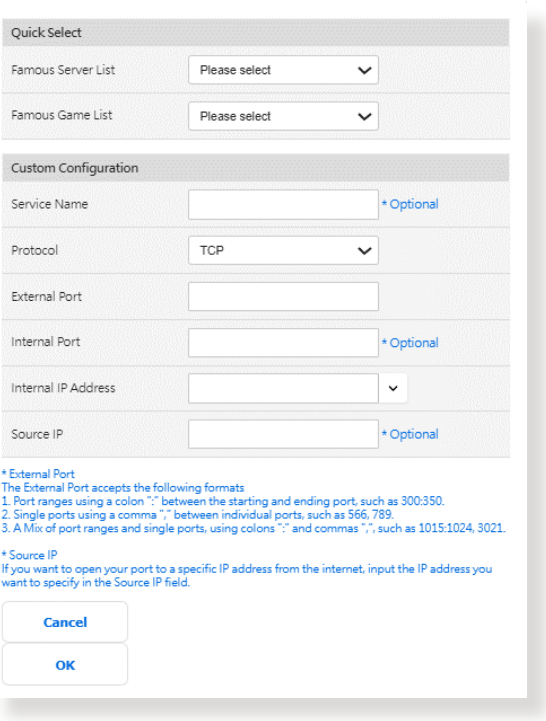
Se pretender especificar um intervalo de portas para clientes na mesma rede, introduza o nome do serviço, o intervalo de portas (por exemplo, 10200:10300), o endereço IP da LAN e deixe a porta local em branco.

NOTA: Quando o reencaminhamento de portas está ativado, o router ASUS bloqueia tráfego de entrada não solicitado a partir da Internet e permite apenas respostas de pedidos de saída a partir da LAN. O cliente de rede não tem acesso direto à Internet e vice-versa.



Para configurar o Reencaminhamento de Portas:

1. No painel de navegação, aceda a **Settings (Definições)** > **WAN** > **Virtual Server / Port Forwarding (Servidor virtual / Reencaminhamento de portas)**.
2. Deslize o interruptor para **ON (Ativado)** para ativar o encaminhamento de portas e, em seguida, clique em **Add Profile (Adicionar perfil)**. Depois de configurar as definições, clique em **OK**.



- **Lista de servidores famosos**: Escolha o tipo de serviço ao qual deseja aceder.
- **Lista de jogos famosos**: Este item apresenta a lista de portas necessárias para que jogos online populares funcionem corretamente.
- **Nome do serviço**: Introduza o nome do serviço.
- **Protocolo**: Selecione o protocolo. Se tiver dúvidas, Selecione **BOTH (AMBOS)**.
- **External Port (Porta externa):** Aceita os seguintes formatos:
  1) Um intervalo de portas separadas com dois pontos "**:**" para especificar os limites superior e inferior do limite, tais como 300:350;
  2) Números de portas individuais separados com vírgula "," para os separar, tais como 566, 789;
  3) Uma mistura de intervalos de portas e portas individuas, separados com dois pontos ":" e vírgulas ",", tais como 1015:1024, 3021.
- **Internal Port (Porta interna)**: Introduza uma porta específica para receber pacotes reencaminhados. Deixe este campo

em branco se deseja que os pacotes recebidos sejam corretamente para o intervalo de portas especificado.

- **Internal IP Address (Endereço IP interno)**: Introduza o endereço IP da LAN do cliente.
- **Source IP (IP de origem):** Se deseja abrir a sua porta para um endereço IP específico da Internet, insira neste campo o endereço IP ao qual deseja aceder.

NOTA: Utilize um endereço IP estático para o cliente local para que o reencaminhamento de portas funcione corretamente. Para mais informações, consulte a secção **3.9 LAN**.

Para verificar se o Reencaminhamento de Portas foi configurado com sucesso:

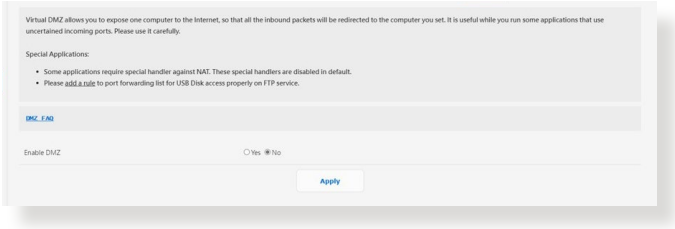
- Certifique-se de que o seu servidor ou aplicação está configurado(a) e em execução.
- Será necessário um cliente fora da sua LAN mas com acesso à Internet (referido como "Cliente de Internet"). Este cliente não deverá estar ligado ao router ASUS.
- No cliente de Internet, utilize o IP da WAN do router para aceder ao servidor. Se o reencaminhamento de portas estiver configurado com sucesso, deverá ser possível aceder aos ficheiros ou aplicações.

Diferenças entre ativação de portas e reencaminhamento de portas:

- A ativação de portas funcionará mesmo que não seja configurado um endereço IP da LAN específico. Ao contrário do reencaminhamento de portas, que necessita de um endereço IP da LAN estático, a ativação de portas permite o reencaminhamento dinâmico de portas utilizando o router. Intervalos de portas predeterminados são configurados para aceitar ligações durante um período de tempo limitado. A ativação de portas permite que vários computadores executem aplicações que, geralmente, necessitam do reencaminhamento manual das mesmas portas para cada PC da rede.
- A ativação de portas é mais segura do que o reencaminhamento de portas, visto que as portas de entrada não estão permanentemente abertas. Essas portas são abertas apenas quando uma aplicação efetua uma ligação de saída através da porta de ativação.

3.17.5 DMZ

A DMZ virtual permite expor um computador à Internet, de modo a que todos os pacotes recebidos sejam redirecionados para o computador definido. É útil quando são executadas algumas aplicações que utilizam portas de entrada incertas. Utilize com cuidado.



Para configurar o serviço DMZ:

1. No painel de navegação, aceda a **Settings (Definições)** > **WAN** > **DMZ**.
2. Configure as definições indicadas abaixo. Quando terminar, clique em **Apply (Aplicar)**.

- **IP address of Exposed Station (Endereço IP da estação exposta):** Introduza o endereço IP da LAN do cliente que irá fornecer o serviço DMZ e ficará exposto na Internet. Certifique-se de que o servidor cliente tem um endereço IP estático.

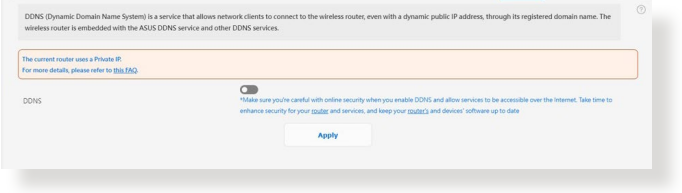
Para remover o serviço DMZ:

1. Elimine o endereço IP da LAN do cliente da caixa de texto **IP Address of Exposed Station (Endereço IP da estação exposta)**.
2. Quando terminar, clique em **Apply (Aplicar)**.

NOTA: Para mais informações, visite https://www.asus.com/support/FAQ/1011723.

3.17.6 DDNS

O DDNS (Dynamic Domain Name System) é um serviço que permite que os clientes da rede liguem ao router com fios, mesmo com um endereço IP público dinâmico, através do seu nome de domínio registado. O router com fios tem incorporado o serviço ASUS DDNS e outros serviços DDNS.



Para configurar o DDNS:

1. No painel de navegação, aceda a **Settings (Definições)** > **WAN** > **DDNS**.
2. Configure as definições indicadas abaixo. Quando terminar, clique em **Apply (Aplicar)**.
   - **Ativar o cliente DDNS**: Active o DDNS para aceder ao router ASUS através do nome DNS em vez do endereço IP da WAN.
   - **Servidor e Nome do anfitrião**: Escolha ASUS DDNS ou outro DDNS. Se deseja utilizar o serviço ASUS DDNS, preencha o Nome do Anfitrião no formato xxx.asuscomm.com (xxx é o nome do seu anfitrião).
   - Se deseja utilizar um serviço DDNS diferente, clique em FREE TRIAL (AVALIAÇÃO GRATUITA) e registe-se online primeiro. Preencha os campos User Name or E-mail Address (Nome de utilizador ou Endereço de e-mail) e Password or DDNS key (Palavra-passe ou Chave DDNS).
   - **Ativar caracteres universais**: Ative os caracteres universais se o seu serviço DDNS o exigir.

NOTAS:

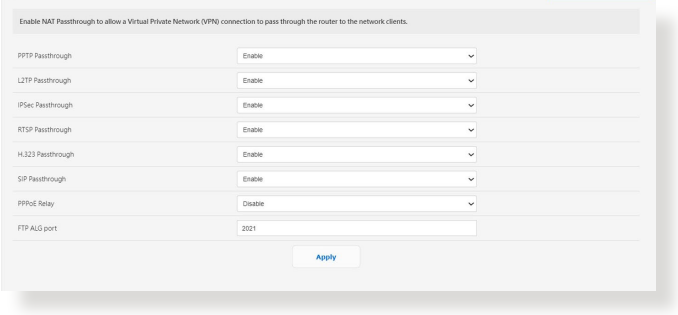
O serviço DDNS não funcionará nas seguintes condições:

- Quando o router com fios estiver a utilizar um endereço IP da WAN privado (192.168.x.x, 10.x.x.x ou 172.16.x.x), indicado por um texto em amarelo.
- O router poderá estar numa rede que utiliza várias tabelas NAT.

3.17.7 Passagem de NAT

Ative a Passagem NAT para permitir que uma Rede Privada Virtual (VPN) passe pelo router para os clientes da rede.

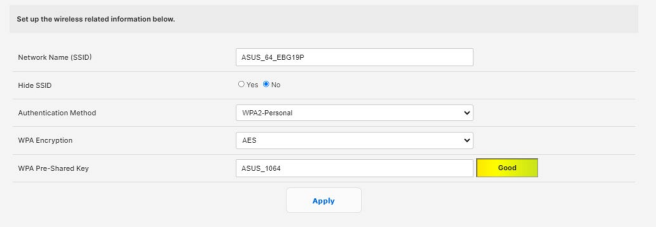
Para configurar a Passagem NAT, aceda a **Settings (Definições)** > **WAN** > **NAT Passthrough (Passagem de NAT)**. Quando terminar, clique em **Apply (Aplicar)**.



3.18 Sem fios

3.18.1 Geral

O separador **General (Geral)** permite-lhe configurar as definições básicas da rede sem fios.



Para configurar as definições básicas da rede sem fios:

1. No painel de navegação, aceda a **Settings (Definições)** > **Wireless (Sem fios)** > **General (Geral)**.
2. Atribua um nome exclusivo ao seu SSID (Service Set Identifier) ou nome de rede para identificar a sua rede sem fios. Os dispositivos Wi-Fi podem identificar e ligar à rede sem fios através do SSID atribuído. Os SSIDs exibidos na faixa de informações serão atualizados quando os novos SSIDs forem guardados nas definições.

IMPORTANTE! Para tornar a função Wi-Fi disponível, integre um ponto de acesso (PA) sem fios, como ExpertWiFi EBA63 ou router, como ExpertWiFi EBR63 ou ExpertWiFi EBM68, na rede AiMesh do EBG19P.

---

3. No campo **Hide SSID (Ocultar SSID)**, Selecione **Yes (Sim)** para impedir que os dispositivos sem fios detectem o seu SSID. Quando esta função estiver ativada, será necessário introduzir manualmente o SSID no dispositivo sem fios para aceder à rede sem fios.
4. Selecione um destes métodos de autenticação:
   - **Sistema aberto**: Esta opção não oferece segurança.
   - **WPA/WPA2/WPA3-Pessoal**: Esta opção oferece um nível de segurança elevado. Pode utilizar WPA (com TKIP) ou

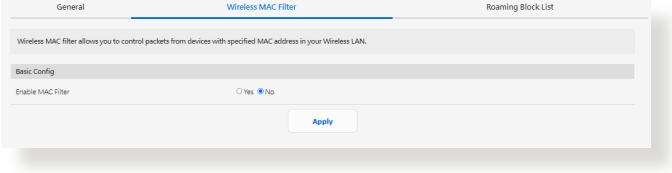
WPA2 (com AES). Se seleccionar esta opção, deverá utilizar a encriptação TKIP + AES e introduzir a frase de acesso WPA (chave de rede).

- **WPA/WPA2/WPA3-Empresarial**: Esta opção oferece um nível de segurança muito elevado. É utilizada com um servidor EAP integrado ou um servidor externo de autenticação back-end RADIUS.

5. Atribua uma palavra-passe única à sua chave WPA previamente partilhada.

3.18.2 Filtro de endereços MAC sem fios

O filtro de endereços MAC sem fios permite controlar os pacotes transmitidos para um determinado endereço MAC (Media Access Control) da sua rede sem fios.

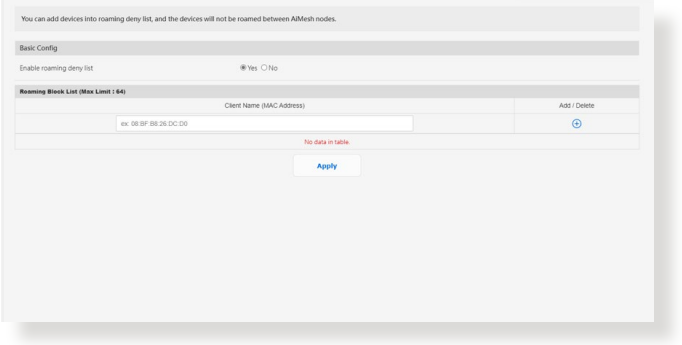


Para configurar o filtro de endereços MAC sem fios:

1. No painel de navegação, aceda a **Settings (Definições)** > **Wireless (Sem fios)** > **Wireless MAC Filter (Filtro de endereços MAC sem fios)**.
2. Marque **Yes (Sim)** no campo **Enable Mac Filter (Ativar Filtro de Mac)**.
3. Na lista pendente **MAC Filter Mode (Modo de filtro de endereços MAC)**, Selecione **Accept (Aceitar)** ou **Reject (Rejeitar)**.
   - Selecione **Accept (Aceitar)** para permitir que os dispositivos da lista de filtro de endereços MAC acedam à rede sem fios.
   - Selecione **Reject (Rejeitar)** para impedir que os dispositivos da lista de filtro de endereços MAC acedam à rede sem fios.
4. Na lista de filtro de endereços MAC, clique no botão ⊕ e introduza o endereço MAC do dispositivo sem fios.
5. Clique em **Apply (Aplicar)**.

3.18.3 Lista de bloqueio de roaming

Esta funcionalidade permite adicionar dispositivos à lista de bloqueio de roaming e impedir que estes façam roaming entre nós AiMesh.



4 Resolução de problemas

Este capítulo apresenta soluções para problemas que poderão ocorrer no seu router. Se ocorrerem problemas não mencionados neste capítulo, visite o site de apoio da ASUS em: https://www.asus.com/support/ para obter mais informações sobre o produto e detalhes de contacto da Assistência Técnica da ASUS.

4.1 Resolução básica de problemas

Se o seu router estiver com problemas, execute os passos indicados nesta secção antes de procurar outras soluções.

Atualize o firmware para a versão mais recente.

1. Aceda à Interface Web do utilizador. Aceda a **Settings (Definições)** > **Administration (Administração)** > **Firmware Upgrade (Atualização do firmware)**. Clique em **Check (Verificar)** para verificar se o firmware mais recente está disponível.
2. Se o firmware mais recente estiver disponível, visite o Web site global da ASUS para transferir o firmware mais recente.
3. Na página **Firmware Upgrade (Atualização do firmware)**, clique em **Browse (Procurar)** para localizar o ficheiro de firmware.
4. Clique em **Upload (Carregar)** para atualizar o firmware.

Reinicie a sua rede na seguinte sequência:

1. Desligue o modem.
2. Retire o cabo de alimentação do modem.
3. Desligue o router e os computadores.
4. Ligue o cabo de alimentação ao modem.
5. Ligue o modem e aguarde 2 minutos.
6. Ligue o router e aguarde 2 minutos.
7. Ligue os computadores.

Verifique se os cabos Ethernet estão corretamente ligados.

- Se o cabo Ethernet que liga o router ao modem estiver corretamente ligado, o LED WAN estará aceso.
- Se o cabo Ethernet que liga o computador ao router estiver corretamente ligado, o respectivo LED LAN estará aceso.

Verifique se as definições da rede estão corretas.

- Todos os clientes da rede deverão ter um endereço IP válido. A ASUS recomenda que utilize o servidor DHCP do router com fios para atribuir endereços IP aos computadores da sua rede.
- Alguns fornecedores de serviço de modem por cabo exigem a utilização do endereço MAC do computador registado inicialmente na conta. Pode ver o endereço MAC na página da Interface Web, **Dashboard (Painel de controlo)** > **Clients (Clientes)**.

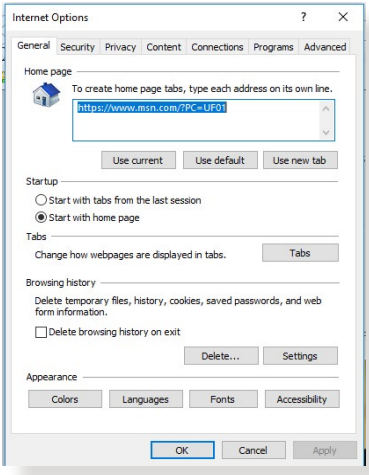
4.2 Perguntas Frequentes (FAQs)

Não consigo aceder à interface de utilizador do router utilizando um navegador Web

- Se o seu computador estiver ligado através de um cabo, verifique a ligação do cabo Ethernet e o LED de estado, tal como descrito na secção anterior.
- Certifique-se que está as informações de início de sessão corretas. Certifique-se de que a tecla Caps Lock está desativada quando introduzir as informações de início de sessão.
- Elimine os cookies e ficheiros do seu navegador Web. No caso do Internet Explorer, siga estes passos:

  1. Abra o Internet Explorer e clique em **Tools (Ferramentas)** > **Internet Options (Opções da Internet)**.

  2. No separador **General (Geral)**, em **Browsing history (Histórico de navegação)**, clique em **Delete… (Eliminar...)**, selecione **Temporary Internet Files and website files (Ficheiros temporários da Internet e ficheiros de websites)** e **Cookies and website data (Cookies e dados de websites)**, depois clique em **Delete (Eliminar)**.



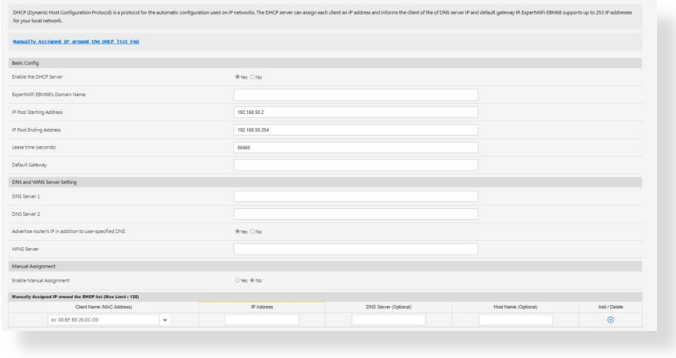
NOTAS:

- Os comandos para eliminar cookies e ficheiros variam de acordo com o navegador Web.
- Desative as definições de servidor proxy, cancele a ligação de acesso telefónico e configure as definições de TCP/IP para obter um endereço IP automaticamente. Para mais detalhes, consulte o Capítulo 1 deste manual do utilizador.
- Certifique-se de que utiliza cabos Ethernet CAT5e ou CAT6.

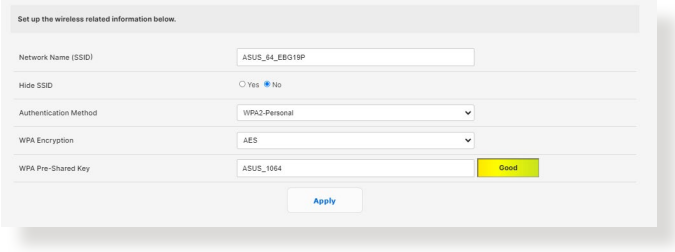
O cliente não consegue estabelecer uma ligação sem fios com o router.

IMPORTANTE! Para tornar a função Wi-Fi disponível, integre um ponto de acesso (PA) sem fios, como ExpertWiFi EBA63 ou router, como ExpertWiFi EBR63 ou ExpertWiFi EBM68, na rede AiMesh do EBG19P.

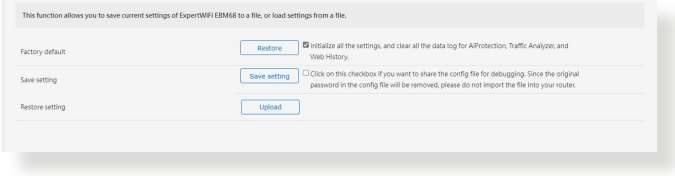
- **O servidor DHCP foi desativado:**
  1. Aceda à Interface Web do utilizador. Aceda a **Dashboard (Painel de controlo)** > **Clients (Clientes)** e procure dispositivos que deseja ligar ao router.
  2. Se não conseguir encontrar o dispositivo no **Dashboard (Painel de controlo)**, aceda a **Settings (Definições)** > **LAN** > **DHCP Server (Servidor DHCP)**.



- O SSID está oculto. Se o seu dispositivo consegue encontrar SSIDs de outros routers mas não consegue encontrar o SSID do seu router, aceda a **Settings (Definições)** > **Wireless (Sem fios)** > **General (Geral)**, selecione **No (Não)** no campo **Hide SSID (Ocultar SSID)**.



- Se estiver a utilizador um adaptador de LAN sem fios, verifique se o canal sem fios em utilização está em conformidade com os canais disponíveis no seu país/área. Caso contrário, ajuste o canal, a largura de banda do canal e o modo sem fios.
- Se continuar sem conseguir ligar ao router com fios, pode repor as predefinições do router. Na interface de utilizador do router, clique em **Settings (Definições)** > **Administration (Administração)** > **Restore/Save/Upload Setting (Restaurar/Guardar/Carregar a Configuração)** e clique em **Restore (Restaurar)**.



Não é possível aceder à Internet

- Verifique se o router consegue ligar ao endereço IP da WAN do seu ISP. Para o fazer, abra a interface Web e aceda a **Dashboard (Painel de controlo)**, e verifique o Estado da Internet.
- Se o router não conseguir ligar ao endereço IP da WAN do seu ISP, experimente reiniciar a sua rede, tal como descrito na secção **Restart your network in following sequence (Reinicie a sua rede na seguinte sequência)** no subcapítulo **Basic Troubleshooting (Resolução básica de problemas)**.
- Se mesmo assim não tiver acesso à Internet, experimente reiniciar o seu computador e verifique o endereço IP e gateway da rede.
- Verifique os indicadores de estado no modem ADSL e no router com fios. Se o LED WAN do router com fios estiver Aceso, verifique se os cabos estão correctamente ligados.

Não se recorda do SSID (nome da rede) ou da palavra-passe da rede

- Configure um novo SSID e uma chave de encriptação através de uma ligação com cabo (cabo Ethernet). Abra a interface Web, aceda a **Dashboard (Painel de controlo)**, clique no ícone do router, introduza um novo SSID e a chave de encriptação e clique em **Apply (Aplicar)**.
- Reponha as predefinições do seu router. Abra a interface Web, aceda a **Settings (Definições)** > **Administration (Administração)** > **Restore/Save/Upload Setting (Restaurar/Guardar/Carregar a Configuração)** e clique em **Restore (Restaurar)**.

Como restaurar o sistema para as predefinições de fábrica?

- Aceda a **Settings (Definições)** > **Administration (Administração)** > **Restore/Save/Upload Setting (Restaurar/Guardar/Carregar a Configuração)** e clique em **Restore (Restaurar)**.

A atualização do firmware falhou.

Inicie o modo de recuperação e execute o utilitário de Restauro do firmware.

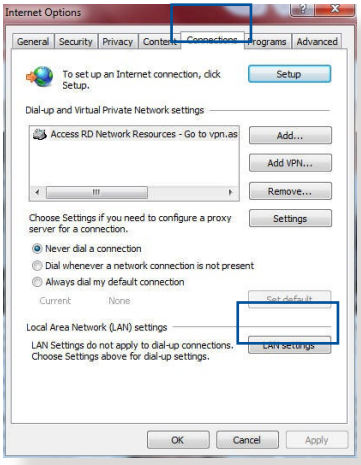
Não é possível aceder à Interface Web

Antes de configurar o seu router com fios, execute os passos descritos nesta secção para o computador anfitrião e clientes de rede.

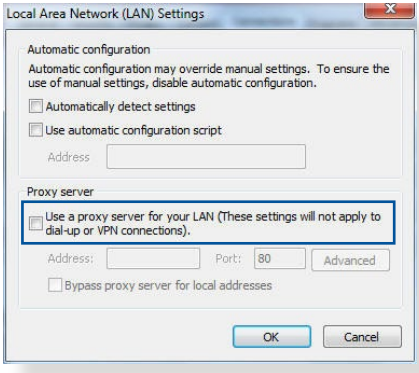
A. Desative o servidor proxy, caso esteja ativado.

Windows®

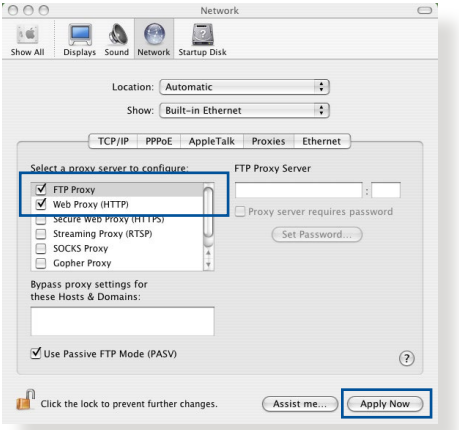
1. Clique em **Start (Iniciar)** > **Internet Explorer** para executar o navegador Web.
2. Clique em **Tools (Ferramentas) > Internet options (Opções da Internet) > Connections (Ligações) > LAN settings (Definições de LAN).**



3. No ecrã Definições de rede local (LAN), desmarque a opção **Use a proxy server for your LAN (Utilizar um servidor proxy para a rede local).**
4. Clique em **OK** quando terminar.



MAC OS



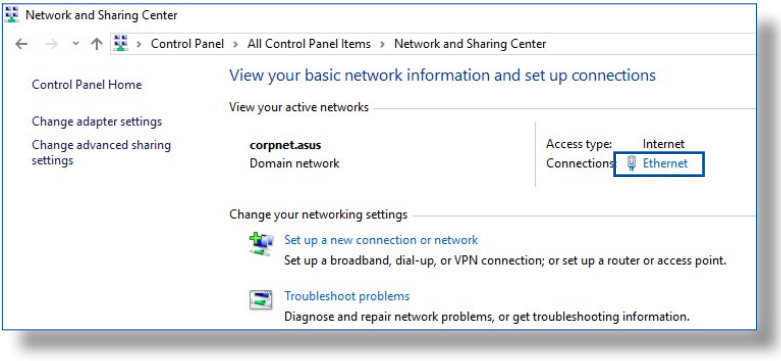
1. No navegador Safari, clique em **Safari > Preferences (Preferências) > Advanced (Avançadas) > Change Settings... (Alterar definições…)**
2. No ecrã Network (Rede), desmarque **FTP Proxy** e **Web Proxy (Proxy Web) (HTTP)**.
3. Clique em **Apply Now (Aplicar agora)** quando terminar.

NOTA: Consulte a ajuda do navegador para obter mais detalhes acerca da desativação do servidor proxy.

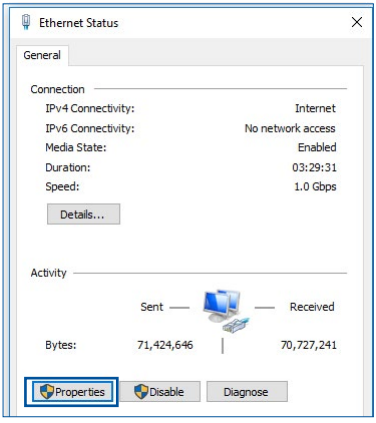
B. Configurar as definições de TCP/IP para obter automaticamente um endereço IP.

Windows®

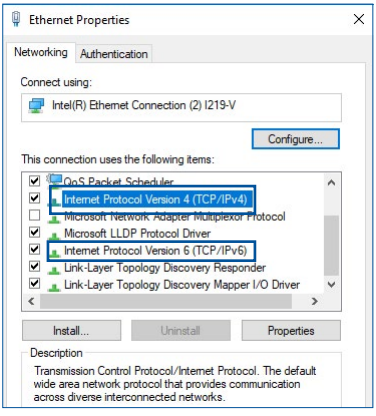
1. Clique em **Start (Iniciar) > Control Panel (Painel de Controlo) > Network and Sharing Center (Centro de Rede e Partilha),** em seguida, clique na ligação de rede para exibir a janela de estado.



2. Clique em **Properties (Propriedades)** para exibir a janela de propriedades de Ethernet.



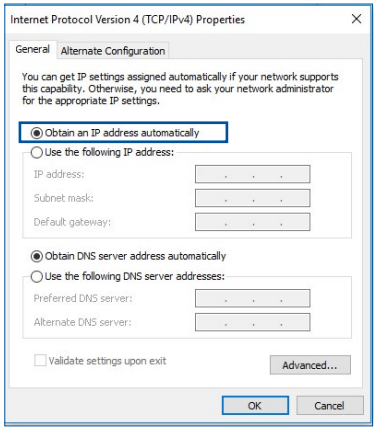
3. Selecione **Internet Protocol Version 4 (TCP/IPv4) (Internet Protocol Versão 4 (TCP/IPv4))** ou **Internet Protocol Version 6 (TCP/IPv6) (Internet Protocol Versão 6 (TCP/IPv6))** depois clique em **Properties (Propriedades).**



4. Para configurar automaticamente as definições de iPv4 IP, marque a opção **Obtain an IP address automatically (Obter automaticamente um endereço IP).**

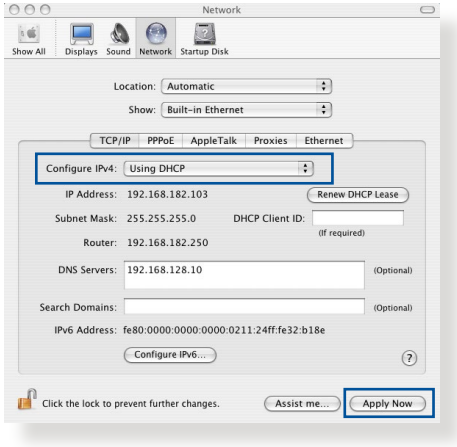
   Para configurar automaticamente as definições de iPv6 IP, marque a opção **Obtain an IPv6 address automatically (Obter automaticamente um endereço IPv6).**

5. Clique em **OK** quando terminar.



MAC OS

1. Clique no ícone Apple no canto superior esquerdo do ecrã.
2. Clique em **System Preferences (Preferências do sistema) > Network (Rede) > Configure... (Configurar…)**
3. No separador **TCP/IP,** Selecione **Using DHCP (Usar DHCP)** na lista pendente **Configure IPv4 (Configurar IPv4)**.



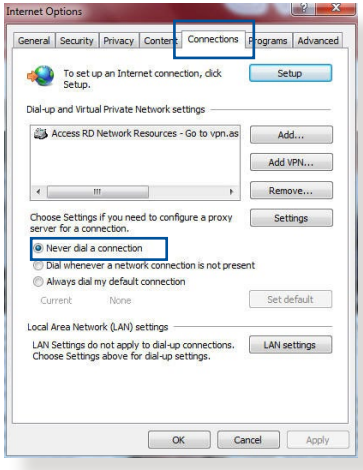
4. Clique em **Apply Now (Aplicar agora)** quando terminar.

NOTA: Consulte a ajuda e suporte do sistema operativo para obter mais detalhes acerca da configuração das definições de TCP/IP do seu computador.

C. Desative a ligação de acesso telefónico, caso esteja ativada.

Windows®

1. Clique em **Start (Iniciar)** > **Internet Explorer** para executar o navegador Web.
2. Clique em **Tool (Ferramentas)** > **Internet Explorer (Opções da Internet)** > **Connections (Ligações).**
3. Marque a opção **Never dial a connection (Nunca marcar para ligar)**.
4. Clique em **OK** quando terminar.



NOTA: Consulte a ajuda do navegador para obter detalhes acerca da desactivação da ligação de acesso telefónico.

Apêndices

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

Avisos de segurança

Quando utilizar este produto, siga sempre as precauções básicas de segurança, incluindo, entre outras, as seguintes:

AVISO!

- O(s) cabo(s) de alimentação deve(m) ser ligado(s) a tomadas elétricas com ligação à terra adequada. Ligue o equipamento apenas a uma tomada elétrica próxima e facilmente acessível.
- Se a fonte de alimentação estiver avariada, não tente repará-la por si próprio. Contacte um técnico qualificado ou o seu revendedor.
- NÃO utilize cabos de alimentação, acessórios ou outros periféricos danificados.
- NÃO instale este equipamento a uma altura superior a 2 metros.
- Utilize este equipamento em ambientes com temperaturas entre 0˚C (32˚F) e 40˚C (104˚F).
- Leia as orientações operacionais e a gama de temperaturas indicadas antes de utilizar o produto.
- Preste atenção especial à segurança pessoal quando utilizar este aparelho em aeroportos, hospitais, estações de serviço e oficinas.
- Interferências com dispositivos médicos: Mantenha uma distância mínima de pelo menos 15 cm entre dispositivos médicos implantados e os produtos ASUS para reduzir o risco de interferências.
- Os produtos ASUS devem ser utilizados com boas condições de receção para reduzir o nível de radiação.
- Mantenha o dispositivo afastado de grávidas e da parte inferior do abdómen de adolescentes.
- NÃO utilize este produto se forem observados defeitos visíveis ou se o mesmo tiver sido molhado, danificado ou modificado. Procure assistência técnica.

AVISO!

- NÃO coloque o computador em superfícies irregulares ou instáveis.
- NÃO coloque nem deixe cair objetos em cima do produto. Evite expor o produto a choques mecânicos, tais como, esmagamento, dobragem, perfuração ou trituração.
- NÃO desmontar, abrir, colocar num micro-ondas, incinerar, pintar ou introduzir quaisquer objetos estranhos neste produto.
- Verifique a etiqueta relativa à tensão na parte inferior do seu dispositivo e assegure-se de que o seu transformador corresponde a essa tensão.
- Manter o produto afastado de fogo e fontes de calor.
- NÃO exponha o equipamento nem o utilize próximo de líquidos, chuva ou humidade. NÃO utilizar o produto durante tempestades elétricas.
- Ligue os circuitos de saída de PoE deste produto exclusivamente a redes PoE, sem encaminhar para instalações externas.
- Para evitar o risco de choque eléctrico, desligue o cabo de alimentação da tomada eléctrica antes de deslocar o sistema.
- Utilize apenas acessórios que tenham sido aprovados pelo fabricante do dispositivo para funcionar com este modelo. A utilização de outros acessórios pode invalidar a garantia ou violar as normas e leis locais, e pode originar riscos de segurança. Contacte o revendedor local para obter informações sobre a disponibilidade de acessórios autorizados.
- A utilização deste produto de uma forma não recomendada nas instruções fornecidas pode originar num risco de incêndio ou de ferimentos.

Assistência E Suporte

Visite nosso site multilingue em https://www.asus.com/support.