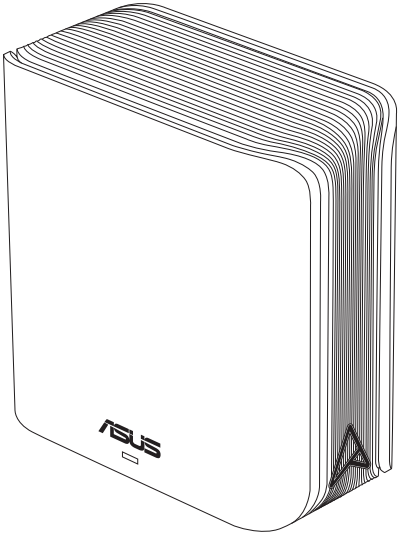
Manual do utilizador

ZenWiFi BD4

BE3600 Roteador de banda dupla



IN SEARCH OF INCREDIBLE

PG23951

Primeira edição

Agosto de 2024

Índice

Índice

Índice

1 Conheça o seu router sem fios

1.1 Bem-vindo!

Obrigado por ter adquirir um Router Sem Fios ASUS ZenWiFi BD4!

Com um toque metálico na cor do monograma A no chassis branco minimalista, o ZenWiFi BD4 oferece ligação de duas bandas 2,4 GHz e 5 GHz para proporcionar incomparáveis transmissões HD sem fios em simultâneo; servidor SMB, servidor UPnP AV e FTP para partilha de ficheiros permanente; uma capacidade de gerir 300.000 sessões; e a Tecnologia Green Network (Rede Ecológica) da ASUS, que oferece uma solução de poupança de energia até 70% superior.

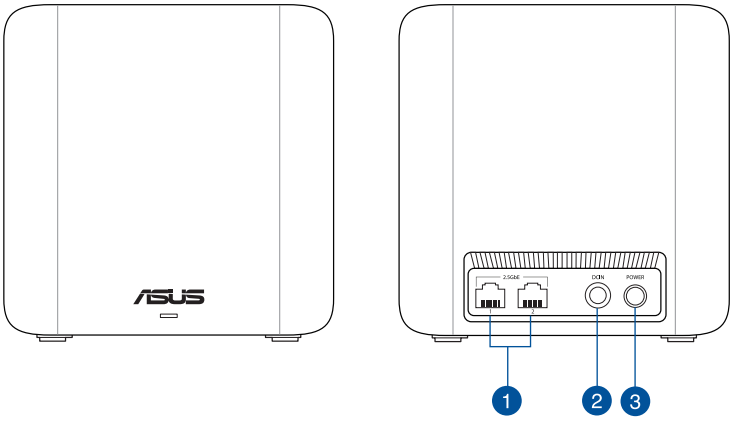
1.2 Conteúdo da embalagem

☑ Router sem fios ZenWiFi BD4
☑ Transformador
☑ Certificado de garantia
☑ Cabo de rede (RJ-45)
☑ Guia de consulta rápida

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 sem fios



1	**Portas 2.5GbE (Deteção automática WAN/LAN)** Ligue os cabos de rede a estas portas para estabelecer uma ligação 2.5GbE WAN/LAN.
2	**Porta de alimentação (Entrada DCIN)** Ligue o transformador AC fornecido a esta porta e ligue o router a uma tomada eléctrica.
3	**Botão de alimentação** Pressione este botão para ligar ou desligar o sistema.

NOTAS:

- Utilize apenas o transformador fornecido com o produto. A utilização de outro transformador poderá danificar o dispositivo.
- **Especificações**:

Transformador DC	Saída DC: +12V com corrente máx. de 1,5A		
Temperatura de funcionamento	0~40°C	Armazenamento	0~70°C
Humidade em funcionamento	50~90%	Armazenamento	20~90%

1.4 Posicionamento do router sem fios

Para garantir a melhor qualidade de transmissão entre o router sem fios e os dispositivos de rede a ele ligados:

- Coloque o router sem fios numa área central para obter a maior cobertura possível sem fios para os seus dispositivos de rede.
- Mantenha o dispositivo afastado de obstruções de metal e de luz solar directa.
- Mantenha o dispositivo afastado de dispositivos Wi-Fi que utilizam apenas a norma 802.11g ou 20MHz, periféricos de computador que utilizam a banda 2,4GHz, dispositivos Bluetooth, telefones sem fios, transformadores, motores de alta resistência, lâmpadas fluorescentes, fornos microondas, frigoríficos e outros equipamentos industriais para evitar interferências ou perdas de sinal.
- 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 ou dois computadores que cumpram os seguintes requisitos:

- Porta Ethernet RJ-45 (LAN) (10Base-T/100Base-TX/1000BaseTX)
- Capacidade de conectividade sem fios IEEE 802.11a/b/g/n/ac/ax
- Um serviço TCP/IP instalado
- Navegador Web, como por exemplo o Internet Explorer, Firefox, Safari ou o Google Chrome

---

NOTAS:

- Se o seu computador não possuir capacidades incorporadas de conectividade sem fios, poderá instalar uma placa WLAN IEEE 802.11a/b/g/n/ac/ax no computador para ligar à rede.
- Devido à tecnologia de banda dupla, o seu router sem fios suporta simultaneamente sinais sem fios nas bandas de 2,4GHz e 5GHz. Isso permite-lhe realizar atividades na Internet, como por exemplo, navegação na Internet, leitura/escrita de mensagens de e-mail utilizando a banda 2.4GHz enquanto reproduz ficheiros de áudio/vídeo de alta definição como filmes ou música utilizando a banda 5GHz.
- Alguns dispositivos IEEE 802.11n que pretende ligar à sua rede poderão não suportar a banda 5GHz. Consulte o manual do utilizador do dispositivo para obter mais informações.
- Os cabos Ethernet RJ-45 utilizados para ligar os dispositivos de rede não deverão exceder 100 metros de comprimento.

IMPORTANTE!

- Algumas placas de rede sem fios poderão ter problemas de conectividade com pontos de acesso WiFi 802.11ax.
- Se tenha problemas de conectividade, atualize o controlador para a versão mais recente. Visite o site oficial do fabricante para obter controladores, atualizações e outras informações.
  - Realtek: https://www.realtek.com/en/downloads
  - Mediatek: https://www.mediatek.com/products/connectivity-and-networking/broadband-wifi
  - Intel: https://downloadcenter.intel.com/

---

2 Começar a utilizar

2.1 Configuração do router

IMPORTANTE!

- Utilize uma ligação com fios durante a configuração do seu router sem fios para evitar possíveis problemas de configuração.
- Antes de configurar o seu router sem 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!

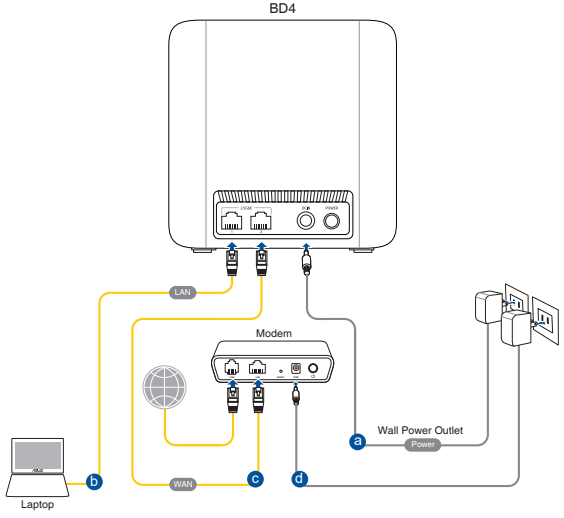
- O(s) cabo(s) de alimentação deve(m) ser ligado(s) a tomadas elétricas com ligação à terra adequada. Ligue o equipamento apenas a uma tomada elétrica próxima e facilmente acessível.
- Se a fonte de alimentação estiver avariada, não tente repará-la por si próprio. Contacte um técnico qualificado ou o 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).

A. 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 sem fios através de uma ligação com fios:

1. Ligue o router a uma tomada elétrica e prima o botão de energia. Ligue o cabo de rede do computador a uma porta 2.5GbE do router.

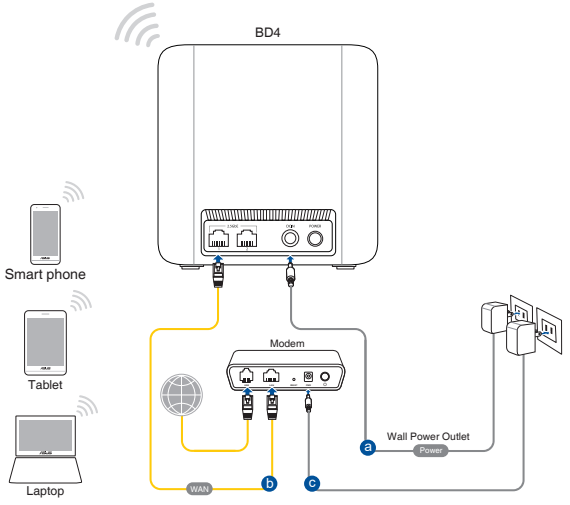


2. A interface web abre automaticamente quando abrir um navegador web. Se não abrir automaticamente, introduza http://www.asusrouter.com.
3. Configure uma palavra-passe para o seu router para impedir o acesso não autorizado.

B. Ligação Sem Fios

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

1. Ligue o router a uma tomada elétrica e prima o botão de energia.



2. Ligue ao nome de rede (SSID) indicado na etiqueta do produto colada na traseira do router. Para uma maior segurança de rede, mude para um SSID exclusivo e defina uma palavra-passe.

Nome da rede Wi-Fi (SSID):	ASUS_XX

* **XX** refere-se aos dois últimos dígitos do endereço MAC 2,4GHz. Pode encontrar esse endereço na etiqueta na traseira do router.

3. Após a ligação, a interface web irá abrir automaticamente quando abrir um navegador web. Se não abrir automaticamente, introduza http://www.asusrouter.com.
4. Configure uma palavra-passe para o seu router para impedir o acesso não autorizado.

NOTAS:

- Para obter detalhes acerca da ligação a uma rede sem fios, consulte o manual do utilizador da placa WLAN.
- Para configurar as definições de segurança da sua rede, consulte a secção **3.1.1 Setting up the wireless security settings (Configurar as definições de segurança da rede sem fios)** deste manual do utilizador.

2.2 Configuração Rápida de Internet (QIS) com detecção automática

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 sem fios para repor as predefinições.

Para utilizar a função QIS com detecção automática:

1. Abra um navegador web. Será redirecionado para o Assistente de Configuração da ASUS (Configuração Rápida da Internet). Caso contrário, aceda manualmente a http://www.asusrouter.com.
2. O router sem fios detecta automaticamente se o tipo de ligação do seu ISP é de **Dynamic IP (IP Dinâmico)**, **PPPoE**, **PPTP** e **L2TP**. Introduza as informações necessárias para o tipo de ligação do seu ISP.

   IMPORTANTE! Contacte o seu ISP, para obter as informações necessárias relativas ao seu tipo de ligação à Internet.

   NOTAS:
   - A detecção automática do tipo de ligação do seu ISP ocorrerá quando configurar o router sem fios pela primeira vez ou quando forem repostas as predefinições do router sem fios.
   - Se a função QIS não detectar o seu tipo de ligação à Internet, clique em **Manual setting (Configuração manual)** e configure manualmente as definições da ligação.

3. Atribua o nome da rede sem fio (SSID) e a chave de segurança para sua conexão sem fio da Rede WiFi 7. Clique em **Apply (Aplicar)** quando terminar.
4. Na página **Login Information Setup (Configuração das informações de início de sessão)**, altere a palavra-passe de início de sessão do router para evitar o acesso não autorizado ao seu router sem fios.

NOTA: Sem fios é diferente do nome da rede (SSID) de WiFi 7 e da chave de segurança. O nome de utilizador e palavra-passe de início de sessão do router sem fios permite-lhe iniciar sessão na Interface Web do router para configurar as definições do router sem fios. O nome da rede (SSID) de WiFi 7 e a chave de segurança permitem que dispositivos Wi-Fi acedam e liguem à sua rede de WiFi 7.

2.3 Ligar à rede sem fios

Depois de configurar o seu router sem fios através da função QIS, pode ligar o computador ou outros dispositivos à sua rede sem fios.

Para ligar à sua rede:

1. No seu computador, clique no ícone de rede  na área de notificação para exibir as redes disponíveis.
2. Selecione a rede sem fios à qual deseja ligar e clique em **Connect (Ligar)**.
3. Poderá ser necessário introduzir a chave de segurança da rede para uma rede sem fios protegida, em seguida, clique em **OK**.
4. Aguarde que o computador estabeleça ligação com êxito à rede sem fios. O estado da ligação será exibido e o ícone de rede apresentará o estado ligado  .

NOTAS:

- Consulte os capítulos seguintes, para obter mais informações sobre a configuração das definições da rede sem fios.
- Consulte o manual do utilizador do seu dispositivo para obter mais informações sobre a ligação do mesmo à sua rede sem fios.

3 Configurar as definições gerais e avançadas

3.1 Iniciar sessão na GUI Web

O seu Router Sem Fios ASUS disponibiliza uma interface gráfica web (GUI) intuitiva que permite configurar facilmente as várias funções através de um navegador web, como o Internet Explorer, Firefox, Safari ou o Google Chrome.

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

Para iniciar sessão na GUI Web:

1. No seu navegador Web, introduza manualmente o endereço IP predefinido do router sem fios: http://www.asusrouter.com.
2. Na página de início de sessão, introduza o nome de utilizador e a palavra-passe que definiu em **2.2 Quick Internet Setup (QIS) with Auto-detection (Configuração Rápida de Internet (QIS) com deteção automática).**
3. Pode agora utilizar a Interface Web para configurar as diversas definições do seu Router Sem Fios ASUS.

* A imagem serve apenas como referência.

NOTA: Quando iniciar sessão na Interface Web pela primeira vez, será automaticamente direccionado para a página de Configuração Rápida de Internet (QIS).

3.1.1 Configurar as definições de segurança da rede sem fios

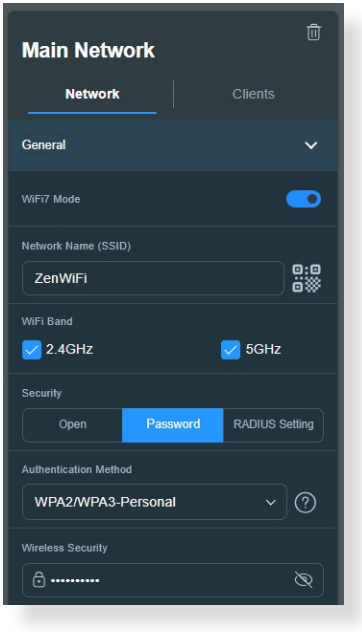
Para proteger a sua rede sem fios contra acessos não autorizados, precisa de configurar as definições de segurança.

Para configurar as definições de segurança da rede sem fios:

1. No painel de navegação, aceda a **General (Geral) > Network Map (Mapa de Rede)**.
2. Selecione a rede e você pode definir as configurações de segurança sem fio, como SSID, nível de segurança e configurações de criptografia.

NOTA: Pode configurar definições de segurança da rede sem fios diferentes para as bandas 2.4GHz e 5GHz.

Definições de segurança 2.4GHz/5GHz



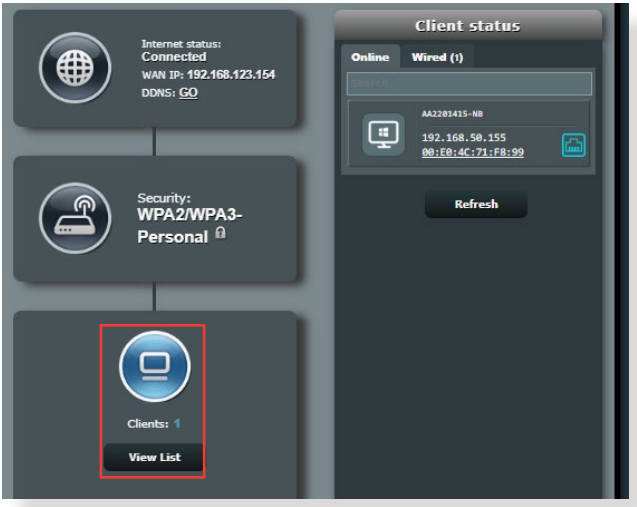
3. No campo **Network Name (SSID) (Nome de rede (SSID))**, introduza um nome exclusivo para a sua rede sem fios.

4. Na lista pendente **WEP Encryption (Encriptação WEP)**, Selecione o método de encriptação para a sua rede sem fios.

IMPORTANTE! A norma IEEE 802.11n/ac/ax proíbe a utilização de débito elevado utilizando WEP ou WPA-TKP como sistema de codificação unicast. Se utilizar estes métodos de encriptação, a velocidade de transmissão de dados diminuirá para 54Mbps utilizando a norma IEEE 802.11g.

5. Introduza a sua chave de acesso de segurança.
6. Clique em **Apply (Aplicar)** quando terminar.

3.1.2 Gerir os clientes da sua rede



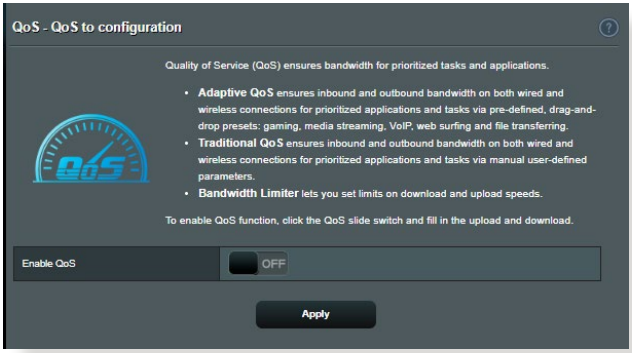
Para gerir os clientes da sua rede:

1. No painel de navegação, aceda a **General (Geral)** > **Network Map (Mapa de Rede)**.
2. No ecrã Network Map (Mapa da rede), selecione o ícone **Client Status (Estado dos clientes)** para exibir as informações acerca dos clientes da sua rede.
3. Para bloquear o acesso de um cliente à sua rede, Selecione o cliente e clique em **block (bloquear).**

3.2 QoS Adaptativo

3.2.1 Gerir a largura de banda de QoS (Qualidade de Serviço)

A Qualidade de Serviço (QoS) permite ajustar a prioridade da largura da banda e gerir o tráfego de rede.



Para configurar a prioridade da largura de banda:

1. No painel de navegação, aceda a **General (Geral)** > **Adaptive QoS (QoS Adaptativo)** > **QoS.**
2. Clique em **ON (Activado)** para ativar a regra predefinida e preencha os campos de largura de banda de envio e transferência.

   NOTA: Solicite ao seu ISP as informações sobre largura de banda.

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

   NOTA: A Lista de Regras Especificadas pelo Utilizador destina-se a definições avançadas. Se deseja atribuir prioridades a aplicações e serviços de rede específicos, Selecione **User-defined QoS rules (Regras QoS definidas pelo utilizador)** ou **User-defined Priority (Prioridade definida pelo utilizador)** na lista pendente no canto superior direito.

4. Na página **user-defined QoS rules (regras definidas pelo utilizador)**, existem quatro tipos de serviço online – navegação na web, HTTPS e transferências de ficheiros. Selecione o serviço preferido, preencha os campos **Source IP or MAC (IP de Origem ou MAC)**, **Destination Port (Porta de destino)**, **Protocol (Protocolo)**, **Transferred (Transferido)** e **Priority (Prioridade)** e clique em **Apply (Aplicar)**. As informações serão configuradas no ecrã de regras QoS.

NOTAS

- Para preencher o IP de origem ou o endereço MAC, poderá:
  a) Introduzir um endereço IP específico como, por exemplo, "192.168.122.1".
  b) Introduzir endereços IP numa sub-rede ou no mesmo conjunto de IP como, por exemplo "192.168.123.*", ou "192.168.*.*"
  c) Introduza todos os endereços IP como "*.*.*.*" ou deixe o campo em branco.
  d) O endereço MAC é composto por seis grupos de dois dígitos hexadecimais, separados por dois pontos (:), na ordem de transmissão (por exemplo, 12:34:56:aa:bc:ef)
- Para o intervalo de portas de origem ou de destino, pode:
  a) Introduzir uma porta específica como, por exemplo, "95".
  b) Introduzir um intervalo de portas como, por exemplo, "103:315", ">100" ou "<65535".
- A coluna **Transferred (Transferido)** contém informações sobre o tráfego enviado e transferido (tráfego de rede enviado e recebido) para uma secção. Nesta coluna, pode definir o limite do tráfego de rede (em KB) para um serviço específico para gerar prioridades para o serviço atribuído a uma porta específica. Por exemplo, se dois clientes de rede, PC 1 e PC 2, estiverem a aceder à Internet (definido na porta 80), mas o PC 1 exceder o limite de tráfego devido a algumas tarefas de transferência, o PC 1 terá uma prioridade mais baixa. Se não pretende definir o limite, deixe em branco.

5. Na página **User-defined Priority (Prioridade definida pelo utilizador)**, pode atribuir prioridade a aplicações ou dispositivos de rede em cinco níveis a partir da lista pendente **user-defined QoS rules (regras QoS definidas pelo utilizador)**. De acordo com o nível de prioridade, pode utilizar os seguintes para enviar pacotes de dados:
   - Altere a ordem dos pacotes de rede enviados para a Internet.
   - Na tabela **Upload Bandwidth (Largura de banda de envio)**, defina **Minimum Reserved Bandwidth (Largura de banda reservada)** e **Maximum Bandwidth Limit (Limite máximo de largura de banda)** para várias aplicações de rede com diferentes níveis de prioridade. As percentagens indicam as taxas de largura de banda para envio disponíveis para aplicações de rede especificadas.

NOTAS:

- Os pacotes de baixa prioridade são ignorados para garantir a transmissão de pacotes de alta prioridade.
- Na tabela **Download Bandwidth (Largura de banda de transferência)**, defina **Maximum Bandwidth Limit (Limite máximo de largura de banda)** para várias aplicações de rede na respectiva ordem. Um pacote de envio com prioridade mais alta originará um pacote de transferência com prioridade mais alta.
- Se nenhum pacote estiver a ser enviado por aplicações de alta prioridade, será utilizada a velocidade total disponível da ligação à Internet para os pacotes de baixa prioridade.

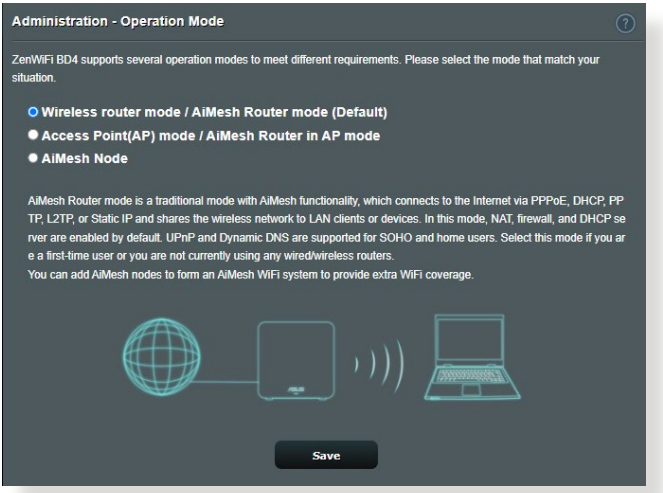
6. Defina o pacote com prioridade mais alta. Para garantir uma experiência de jogos online sem problemas, pode definir ACK, SYN e ICMP como o pacote com prioridade mais alta.

NOTA: Active previamente a função QoS e defina os limites de velocidade de envio e transferência.

3.3 Administração

3.3.1 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 **Advanced Settings (Definições avançadas)** > **Administration (Administração)** > **Operation Mode (Modo de funcionamento)**.
2. Selecione um dos seguintes modos de funcionamento:
   - **Wireless router mode (default) (Modo de router sem fios (predefinido))**: No modo de router sem fios, o router liga à Internet e oferece acesso à Internet a dispositivos disponíveis na sua rede local.
   - **Access Point mode (Modo de ponto de acesso)**: Neste modo, o router cria uma nova rede sem fios na rede existente.
   - **AiMesh Node (Nó AiMesh):** É possível configurar o ZenWiFi BD4 como nó AiMesh para alargar a cobertura de WiFi de routers AiMesh existentes.
3. Clique em **Save (Guardar)**.

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

3.3.2 Sistema

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

Para configurar as definições do sistema:

1. No painel de navegação, aceda a **Advanced Settings (Definições avançadas)** > **Administration (Administração)** > **System (Sistema)**.
2. Pode configurar as seguintes definições:
   - **Change router login password (Alterar a palavra-passe de início de sessão do router)**: Pode alterar a palavra-passe e o nome de início de sessão do router sem fios introduzindo um novo nome e palavra-passe.
   - **WPS button behavior (Comportamento do botão WPS)**: O botão físico WPS do router sem fios pode ser utlizado para ativar a função WPS.
   - **Time Zone (Fuso horário):** Selecione o fuso horário da sua rede.
   - **NTP Server (Servidor NTP)**: O router sem fios pode aceder a um servidor NTP (Protocolo de Hora de Rede) para sincronizar a hora.
   - **Enable Telnet (Ativar Telnet)**: Clique em **Yes (Sim)** para Ativar os serviços Telnet na rede. Clique em **No (Não)** para desativar o serviço Telnet.
   - **Authentication Method (Método de autenticação)**: Pode seleccionar HTTP, HTTPS ou ambos os protocolos para proteger o acesso ao router.
   - **Enable Web Access from WAN (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 sem fios. Selecione **No (Não)** para impedir o acesso.
   - **Only allow specific IP (Permitir apenas IP específicos)**: 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 sem fios a partir da WAN.
3. Clique em **Apply (Aplicar)**.

3.3.3 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 **Advanced Settings (Definições avançadas)** > **Administration (Administração)** > **Firmware Upgrade (Atualização do firmware)**.
2. No campo **Firmware Version (Versão de firmware)**, clique em **Check (Verificar)** 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 sem fios entra automaticamente no modo de emergência ou de falha e o LED indicador de alimentação existente no painel frontal começa a piscar lentamente. Para recuperar ou restaurar o sistema, consulte a secção **4.2 Restauro do firmware**.

3.3.4 Restaurar/Guardar/Transferir as definições

Para restaurar/guardar/transferir as definições:

1. No painel de navegação, aceda a **Advanced Settings (Definições avançadas)** > **Administration (Administração)** > **Restore/Save/Upload Setting (Restaurar/Guardar/Carregar a Configuração)**.
2. Selecione as tarefas que pretende executar:
   - Para restaurar as predefinições de fábrica, clique em **Restore (Restaurar)** e depois em **OK** na mensagem de confirmação.
   - Para guardar as definições do sistema, clique em **Save setting (Guardar definição)**, navegue para a pasta onde deseja guardar o ficheiro e clique em **Save (Guardar)**.
   - Para restaurar as definições do sistema anteriores, clique em **Upload (Transferir)** para procurar o ficheiro de sistema que quer restaurar e depois clique em **Open (Abrir).**

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

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

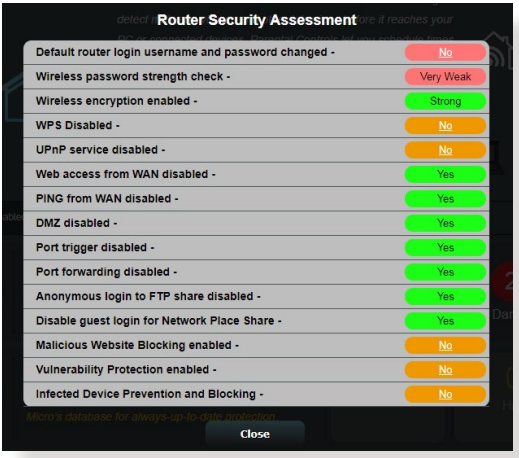
A Protecção de rede impede falhas de segurança de rede e protege-a contra acessos não autorizados.

Configurar a Protecção de rede

Para configurar a Protecção de rede:

1. No painel de navegação, aceda a **General (Geral)** > **AiProtection**.
2. Na página principal do **AiProtection**, clique em **Network Protection (Protecção de rede)**.
3. No separador **Network Protection (Protecção de rede),** clique em **Scan (Pesquisar)**.

   Quando a pesquisa terminar, o utilitário apresenta os resultados na página **Router Security Assessment (Avaliação de segurança do router).**



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), Weak (Fraco)** ou **Very Weak (Muito fraco),** recomendamos que os configure correctamente.

4. (Opcional) Na página **Router Security Assessment (Avaliação de segurança do router)**, configure manualmente os itens assinalados como **No (Não), Weak (Fraco)** ou **Very Weak (Muito fraco)**. 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.

5. Para configurar automaticamente as definições de segurança, clique em **Secure Your Router (Proteger o seu router).**
6. Quando for apresentado uma mensagem de aviso, clique em **OK**.

Bloqueio de sites maliciosos

Esta funcionalidade restringe o acesso a Web sites maliciosos conhecidos na base de dados na nuvem, proporcionando-lhe uma protecção actualizada constantemente.

NOTA: Esta função é activada automaticamente se executar a **Router Weakness Scan (Pesquisa de fragilidades do router).**

Para activar o bloqueio de sites maliciosos:

1. No painel de navegação, aceda a **General (Geral) > AiProtection.**
2. Na página principal do **AiProtection**, clique em **Network Protection (Protecção de rede)**.
3. No painel **Malicious Sites Blocking (Bloqueio de sites maliciosos)**, clique em **ON (Activar).**

IPS bidirecional

O IPS (Sistema de Prevenção de Intrusão) bidirecional protege o seu router contra ataques de rede, bloqueando a receção de pacotes maliciosos e detetando o envio de pacotes suspeitos.

NOTA: Esta função é activada automaticamente se executar a **Router Weakness Scan (Pesquisa de fragilidades do router).**

Para activar a Two-Way IPS (IPS bidirecional):

1. No painel de navegação, aceda a **General (Geral) > AiProtection.**
2. Na página principal do **AiProtection**, clique em **Network Protection (Protecção de rede)**.
3. No painel **Two-Way IPS (IPS bidirecional),** clique em **ON (Activar).**

Prevenção e bloqueio de dispositivos infectados

Esta funcionalidade impede que dispositivos infectados comuniquem informações pessoais ou o estado de infecção a entidades externas.

NOTA: Esta função é activada automaticamente se executar a **Router Weakness Scan (Pesquisa de fragilidades do router).**

Para activar a Protecção de vulnerabilidades:

1. No painel de navegação, aceda a **General (Geral) > AiProtection.**
2. Na página principal do **AiProtection**, clique em N**etwork Protection (Protecção de rede)**.
3. No painel **Infected Device Prevention and Blocking (Prevenção e bloqueio de dispositivos infectados)**, clique em **ON (Activar).**

Para configurar as Preferências de alerta:

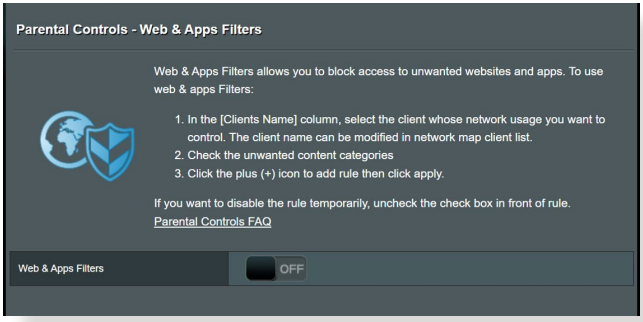
1. No painel **Infected Device Prevention and Blocking (Prevenção e bloqueio de dispositivos infectados),** clique em **Alert Preference (Preferências de alerta)**.
2. Seleccione ou introduza o fornecedor de correio electrónico, a conta de e-mail e palavra-passe e clique em **Apply (Aplicar).**

3.4.2 Configurar o Controlo parental

O Controlo parental permite-lhe controlar o tempo de acesso à Internet ou definir um limite de tempo para a utilização da rede de um cliente.

Para aceder à página principal do Controlo parental:

No painel de navegação, aceda a **General (Geral) > Parental Controls (Controlo parental).**



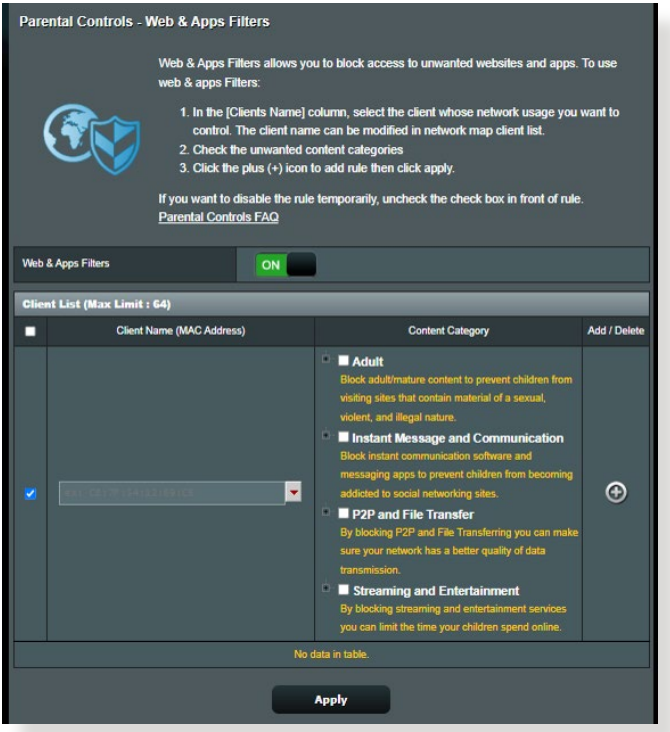
Filtros Web e de aplicações

Os Filtros Web e de aplicações são uma funcionalidade do **Parental Controls (Controlo parental)** que lhe permite bloquear o acesso a Web sites ou aplicações não desejados.

Para configurar os Filtros Web e de aplicações:

1. No painel de navegação, aceda a **General (Geral) > Parental Controls (Controlo parental).**
2. No painel **Web & Apps Filters (Filtros Web e de aplicações)**, clique em **ON (Activar)**.
3. Quando for apresentada a mensagem do Acordo de Licença do Utilizador Final (EULA), clique em **I agree (Concordo)** para continuar.
4. Na coluna **Client List (Lista de clientes)**, seleccione ou introduza o nome do cliente a partir da caixa de lista pendente.

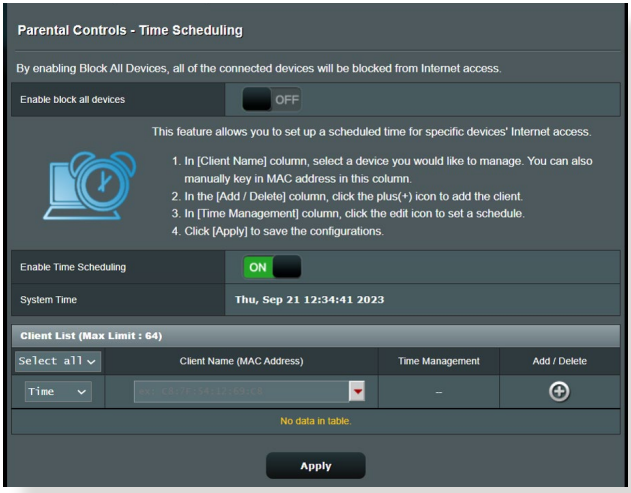
5. Na coluna **Content Category (Categoria dos conteúdos)**, seleccione os filtros nas quatro categorias principais: **Adult (Adulto), Instant Message and Communication (Mensagens instantâneas e comunicação), P2P and File Transfer (P2P e transferência de ficheiros)** e **Streaming and Entertainment (Transmissão e entretenimento).**
6. Clique em ⊕ para adicionar o perfil do cliente.
7. Clique em **Apply (Aplicar)** para guardar as definições.



Time Scheduling (Agendamento)

O Agendamento permite-lhe definir o limite de tempo de utilização da rede para um cliente.

NOTA: Certifique-se de que a hora do seu sistema está sincronizada com o servidor NTP.



Para configurar o Agendamento:

1. No painel de navegação, aceda a **General (Geral) > Parental Controls (Controlo parental) > Time Scheduling (Agendamento).**
2. No painel **Enable Time Scheduling (Activar agendamento),** clique em **ON (Activar).**
3. Na coluna **Clients Name (Nome do cliente)**, seleccione ou introduza o nome do cliente a partir da caixa de lista pendente.

   NOTA: Pode também introduzir o endereço MAC do cliente na coluna **Client MAC Address (Endereço MAC do cliente).** Certifique-se de que o nome do cliente não contém caracteres especiais nem espaços, já que estes poderão causar funcionamento anormal do router.

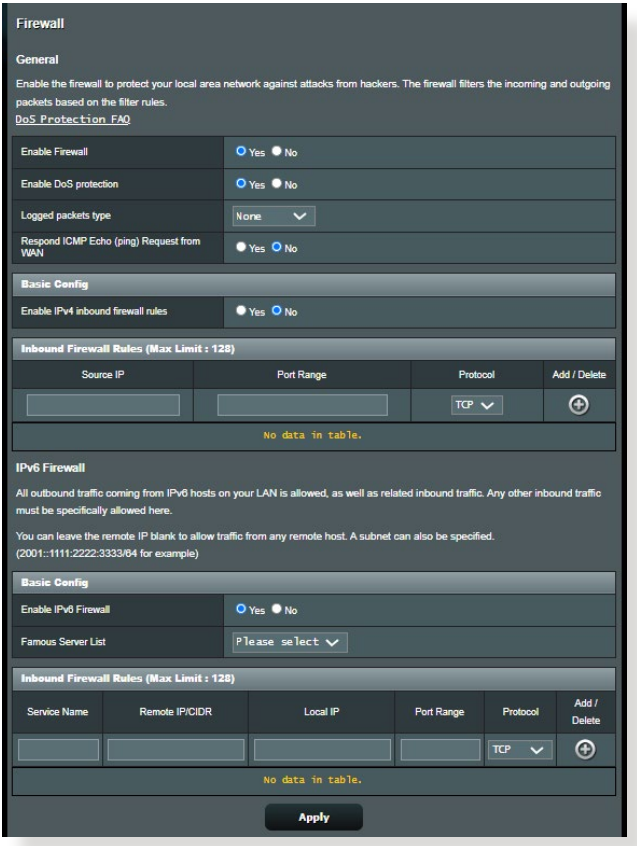
4. Clique em ⊕ para adicionar o perfil do cliente.
5. Clique em **Apply (Aplicar)** para guardar as definições.

3.5 Firewall

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

NOTA: Esta funcionalidade de firewall está ativada por predefinição.

3.5.1 Geral



Para configurar as definições básicas da firewall:

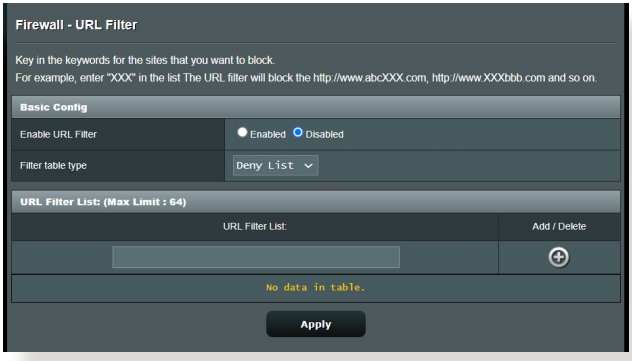
1. No painel de navegação, aceda a **Advanced Settings (Definições avançadas)** > **Firewall** > **General (Geral)**.
2. No campo **Enable Firewall (Ativar firewall)**, selecione **Yes (Sim).**

3. No campo **Enable DoS protection (Ativar protecção DoS)**, 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)**.

3.5.2 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.

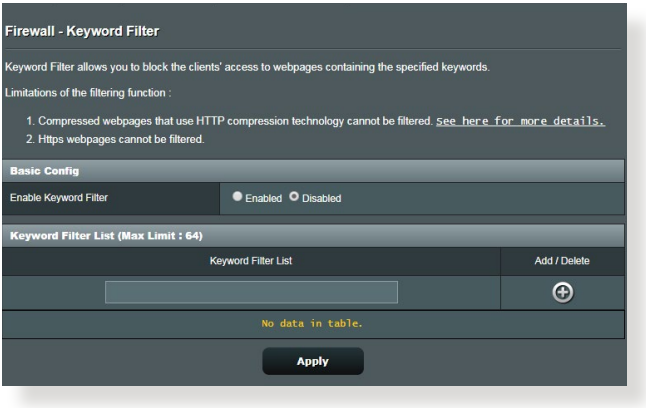


Para configurar um filtro de URL:

1. No painel de navegação, aceda a **Advanced Settings (Definições avançadas)** > **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)**.

3.5.3 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:

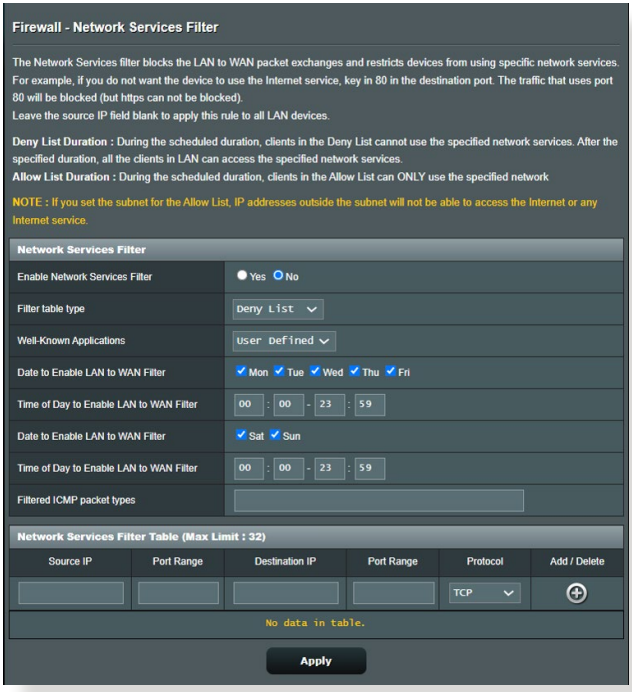
1. No painel de navegação, aceda a **Advanced Settings (Definições avançadas)** > **Firewall** > **Keyword Filter (Filtro de palavra-chave)**.
2. No campo Enable Keyword Filter (Ativar filtro de palavra-chave), Selecione **Enabled (Ativado)**.
3. Introduza uma palavra ou frase e clique no botão **Add (Adicionar)**.
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.

3.5.4 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 **Advanced Settings (Definições avançadas)** > **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 (Recusar)** bloquei os serviços de rede especificados. A **Allow (Permitir)** 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)**.

3.6 IPv6

Este router sem fios suporta o endereçamento IPv6, um sistema que suporta mais endereços IP. Esta norma ainda não está amplamente disponível. 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 **Advanced Settings (Definições avançadas)** > **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)**.

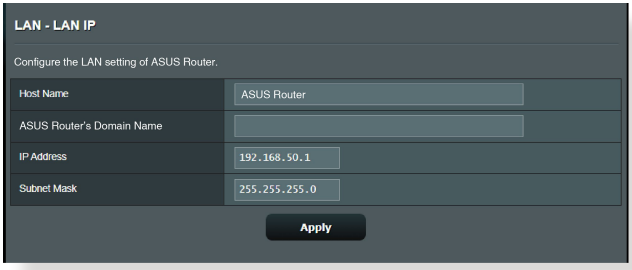
NOTA: Consulte o seu ISP para obter informações específicas sobre IPv6 para o seu serviço de Internet.

3.7 LAN

3.7.1 IP da LAN

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

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

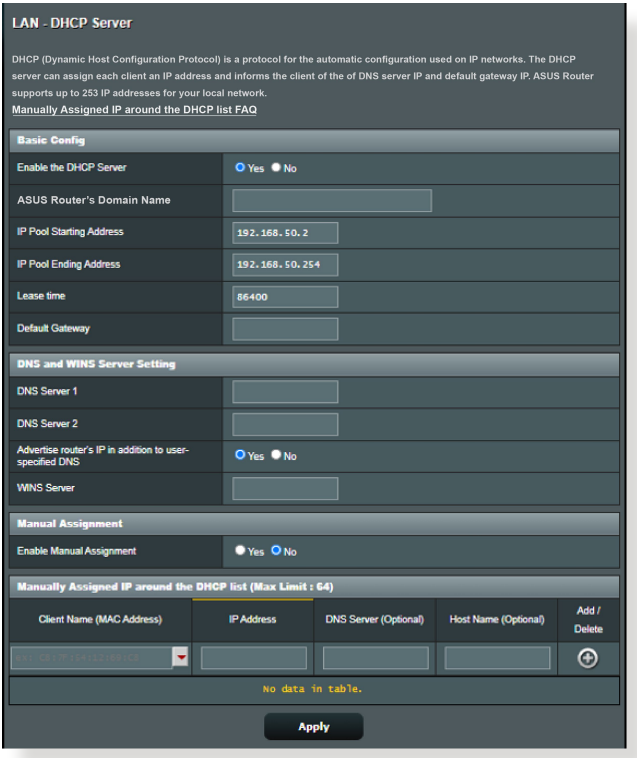


Para modificar as definições de IP da LAN:

1. No painel de navegação, aceda a **Advanced Settings (Definições avançadas)** > **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)**.

3.7.2 DHCP Server

O seu router sem fios utiliza DHCP para atribuir automaticamente endereços IP na sua rede. Pode especificar o intervalo de endereços IP e o tempo de concessão para os clientes da sua rede.



Para configurar o servidor DHCP:

1. No painel de navegação, Clique em **Advanced Setting (Definições avançadas)** > **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 sem 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:

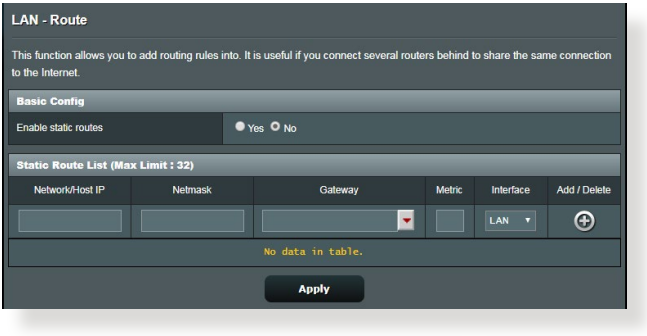
- Recomendamos que utilize um endereço IP no formato 192.168.50.xxx (sendo que xxx pode ser qualquer número entre 2 e 254) quando especificar um intervalo de endereços IP.
- O endereço inicial do conjunto de IP não deverá ser superior ao endereço final do conjunto de IP.

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 sem 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.

3.7.3 Encaminhamento

Se a sua rede utiliza mais do que um router sem fios, pode configurar uma tabela de encaminhamento para partilhar o mesmo serviço de Internet.

NOTA: Recomendamos que não altere as predefinições de encaminhamento se não tem conhecimentos avançados sobre tabelas de encaminhamento.

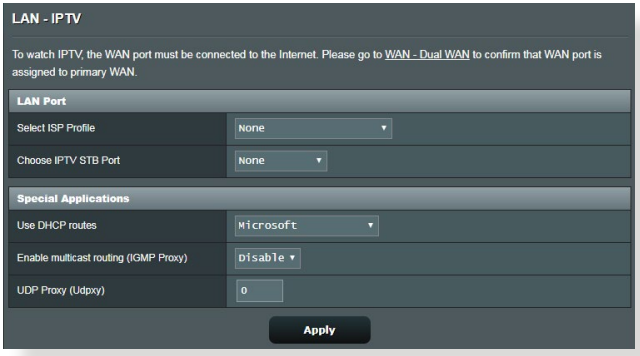


Para configurar a tabela de encaminhamento da LAN:

1. No painel de encaminhamento, aceda a **Advanced Settings (Definições avançadas)** > **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 **Add (Adicionar)** ou **Delete (Eliminar)** para adicionar ou remover um dispositivo da lista.
4. Clique em **Apply (Aplicar)**.

3.7.4 IPTV

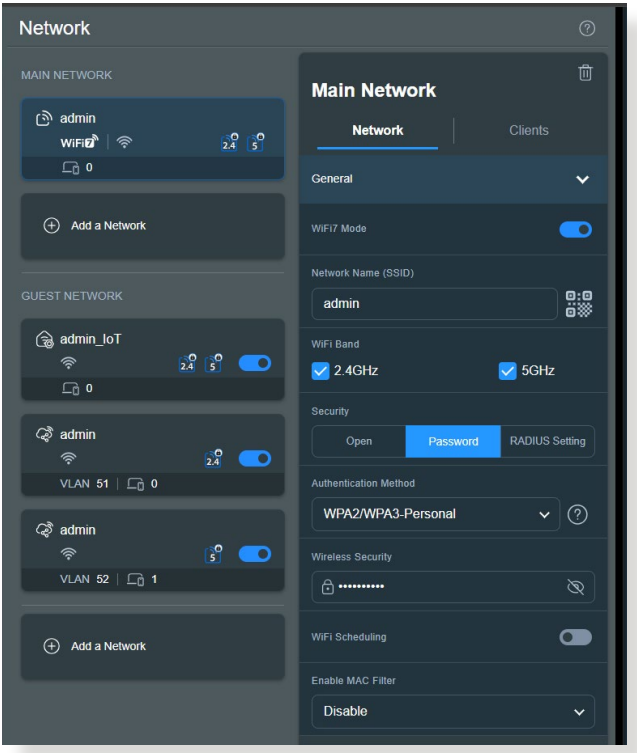
O router sem fios suporta a ligação a serviços de IPTV através de um ISP ou uma LAN. O separador IPTV disponibiliza definições de configuração para IPTV, VoIP, multicasting e UDP para o seu serviço. Contacte o seu ISP para obter as informações específicas sobre o seu serviço.



3.8 Rede

3.8.1 Rede principal - Filtro MAC

Wireless MAC filter provides control over packets transmitted to a specified MAC (Media Access Control) address on your wireless network.



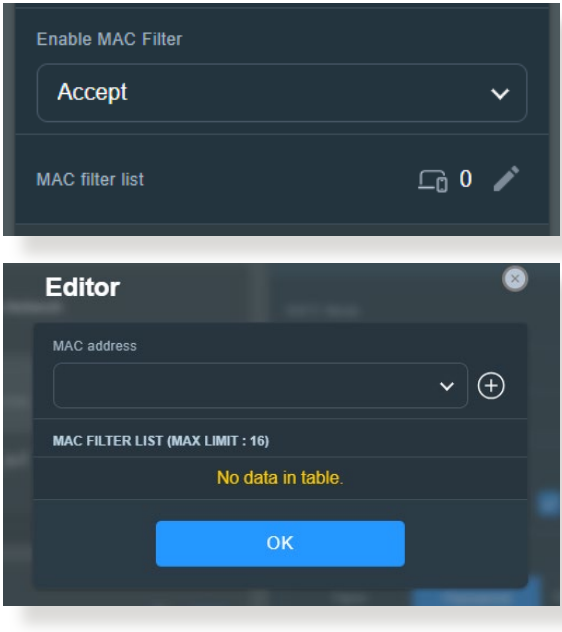
Para configurar o filtro de endereços MAC sem fios:

1. No painel de navegação, aceda a **General (Geral) > Network (Rede) > Main Network (Rede principal)** e selecione o nome da rede (SSID) da rede principal.
2. Na lista pendente **Enable Mac Filter (Ativar Filtro de 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.

NOTA: Selecione **Disable (Desativar)** se quiser desativar **Enable MAC Filter (Ativar Filtro MAC)**.

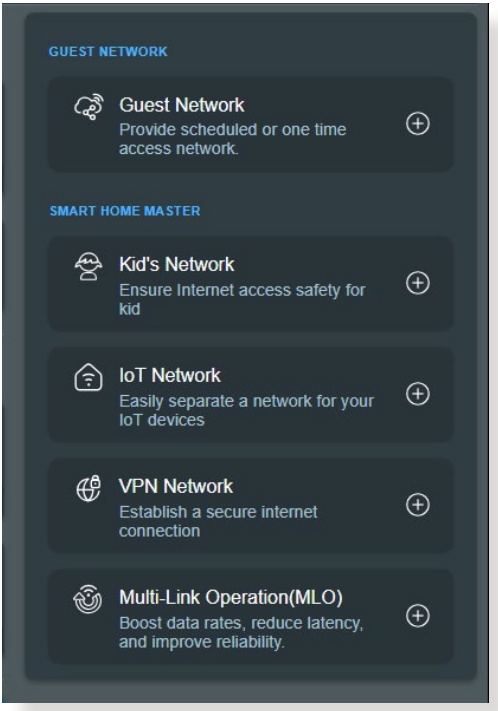
4. Na lista de filtro de endereços MAC, clique em para aceder à página **Editor** e, em seguida, clique em e introduza o endereço MAC do dispositivo sem fios.
5. Clique em **OK**.



3.8.2 Rede de Convidados

3.8.2.1 Rede de Convidados

A Rede de Convidados oferece ligação à Internet para visitantes temporários através do acesso a SSIDs ou redes independentes sem fornecer acesso à sua rede privada.

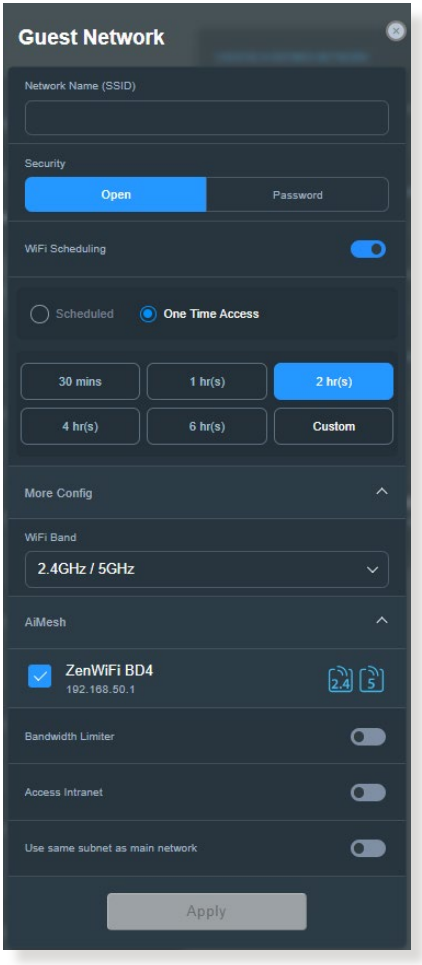


NOTA: O ZenWiFi BD4 suporta até três SSIDs na Rede de Convidados.

Para criar uma rede de convidados:

1. No painel de navegação, aceda a **General (Geral)** > **Network (Rede) > Guest Network (Rede de Convidados)** > **Add a Network (Adicionar uma rede)**.
2. Selecione **Guest Network (Rede de Convidados)** e atribua um nome de rede para sua rede temporária no campo **Network Name (Nome da Rede) (SSID)**.
3. Selecione um método de autenticação em **Security (Segurança)**.
4. Especifique o horário de acesso ou escolha **Scheduled (Agendado)** para adicionar um perfil de agendamento online.

5. Selecione a **WiFi Band (Banda WiFi)** para a rede de convidados que você deseja criar.
6. Habilite ou desabilite o **Bandwidth Limiter (Limitador de Largura de Banda)**.
7. Habilite ou desabilite a **Access Intranet (Intranet de Acesso)**.
8. Quando terminar, clique em **Apply (Aplicar)**.

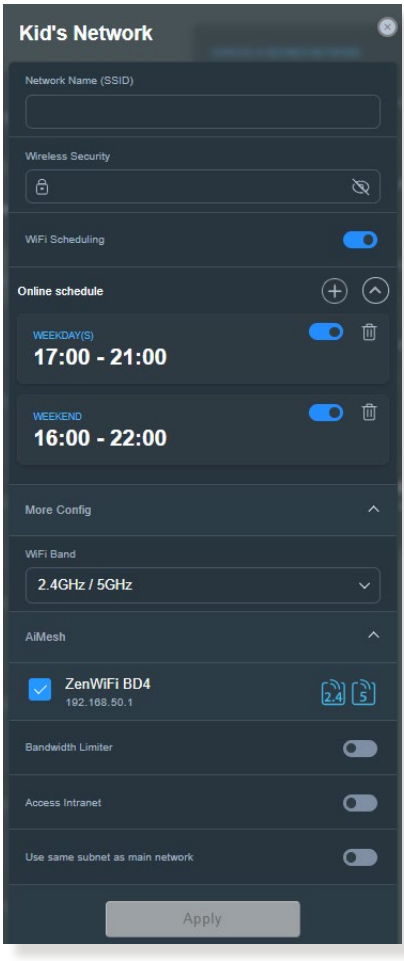


3.8.2.2 Smart Home Master

O Smart Home Master é uma ferramenta poderosa e intuitiva para segmentação de redes. Simplifica o processo de criação e gestão de cenários avançados de sub-redes, como a criação de um SSID dedicado para dispositivos dos seus filhos, ligação a uma VPN através de uma sub-rede dedicada, ou mesmo, a criação de um SSID seguro para todos os seus dispositivos IoT.

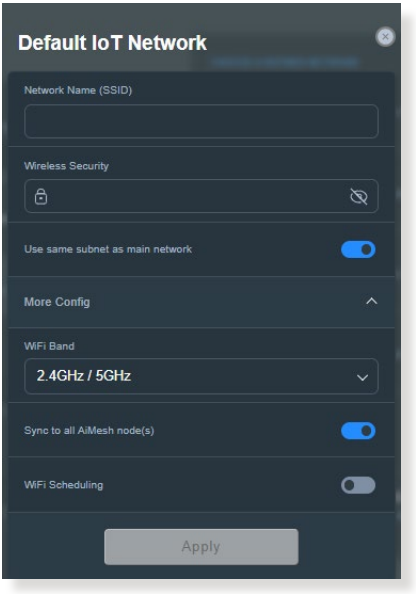
Para criar uma rede infantil:

1. No painel de navegação, aceda a **General (Geral)** > **Network (Rede) > Guest Network (Rede de Convidados)** > **Add a Network (Adicionar uma rede)**.
2. Selecione **Kid's Network (Rede infantil)** e atribua um nome de rede e uma chave de segurança nos campos **Network Name (Nome da Rede) (SSID)** e **Wireless Security (Segurança sem fio)**.
3. Personalize o tempo de acesso à Internet no campo **Online schedule (Agendamento online)**.
4. Selecione a **WiFi Band (Banda WiFi)** para a rede infantil que você deseja criar.
5. Habilite ou desabilite o **Bandwidth Limiter (Limitador de Largura de Banda)**.
6. Habilite ou desabilite a **Access Intranet (Intranet de Acesso)**.
7. Quando terminar, clique em **Apply (Aplicar)**.



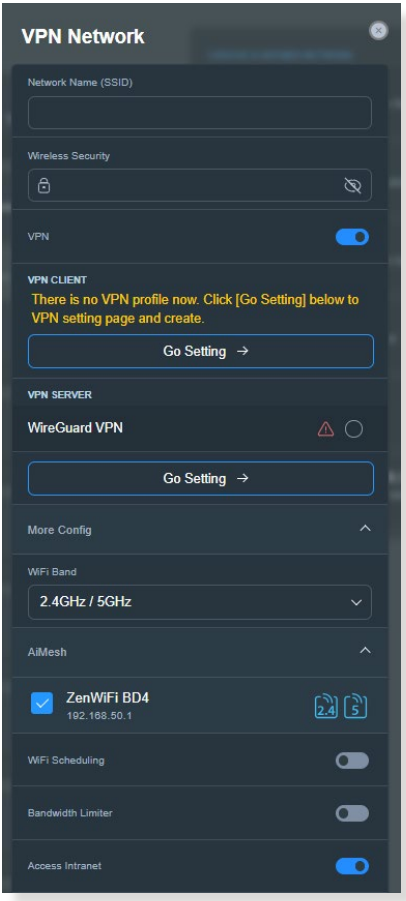
Para criar uma rede IoT:

1. No painel de navegação, aceda a **General (Geral)** > **Network (Rede) > Guest Network (Rede de Convidados)** > **Add a Network (Adicionar uma rede)**.
2. Selecione **IoT Network (Rede IoT)** e atribua um nome de rede e uma chave de segurança nos campos **Network Name (Nome da Rede) (SSID)** e **Wireless Security (Segurança sem fio)**.
3. Selecione a **WiFi Band (Banda WiFi)** para a rede IoT que você deseja criar.
4. Personalize o tempo de acesso à Internet ativando o **WiFi Scheduling (Agendamento de WiFi)**.
5. Quando terminar, clique em **Apply (Aplicar)**.



Para criar uma rede VPN:

1. No painel de navegação, aceda a **General (Geral)** > **Network (Rede) > Guest Network (Rede de Convidados)** > **Add a Network (Adicionar uma rede)**.
2. Selecione **VPN Network (Rede VPN)** e atribua um nome de rede e uma chave de segurança nos campos **Network Name (Nome da Rede) (SSID)** e **Wireless Security (Segurança sem fio)**.
3. Se você não configurou um perfil VPN para o servidor VPN ou cliente VPN, clique em **Go Setting (Ir Configuração)** para criar um perfil VPN.
4. Selecione a **WiFi Band (Banda WiFi)** para a rede VPN que você deseja criar.
5. Personalize o tempo de acesso à Internet ativando o **WiFi Scheduling (Agendamento de WiFi)**.
6. Habilite ou desabilite o **Bandwidth Limiter (Limitador de Largura de Banda)**.
7. Habilite ou desabilite a **Access Intranet (Intranet de Acesso)**.
8. Quando terminar, clique em **Apply (Aplicar)**.


VPN Network
Network Name (SSID)
Wireless Security
VPN
VPN CLIENT
There is no VPN profile now. Click [Go Setting] below to VPN setting page and create.
Go Setting →
VPN SERVER
WireGuard VPN
Go Setting →
More Config
WiFi Band
2.4GHz / 5GHz
AiMesh
ZenWiFi BD4
192.168.50.1
WiFi Scheduling
Bandwidth Limiter
Access Intranet

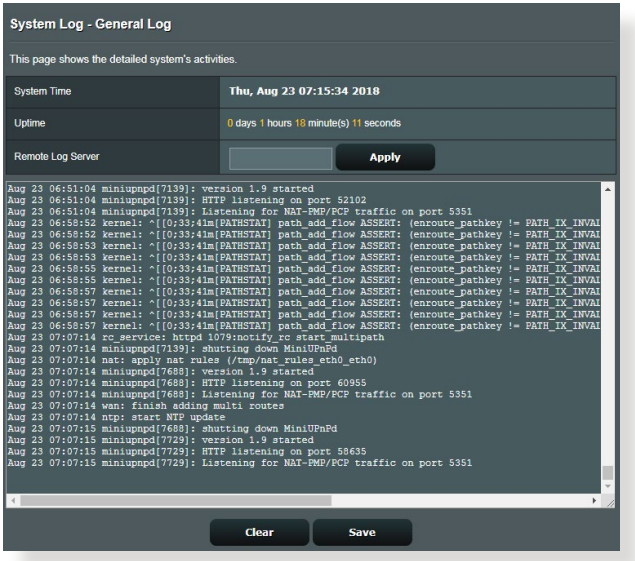
3.9 Registo do sistema

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 **Advanced Settings (Definições avançadas)** > **System Log (Registo do sistema)**.
2. Pode ver as atividades da sua rede em quaisquer dos seguintes separadores:
   - Registo geral
   - Registo sem fios
   - Concessões DHCP
   - IPv6
   - Tabela de encaminhamento
   - Reencaminhamento de portas
   - Ligações



3.10 Analisador de Tráfego

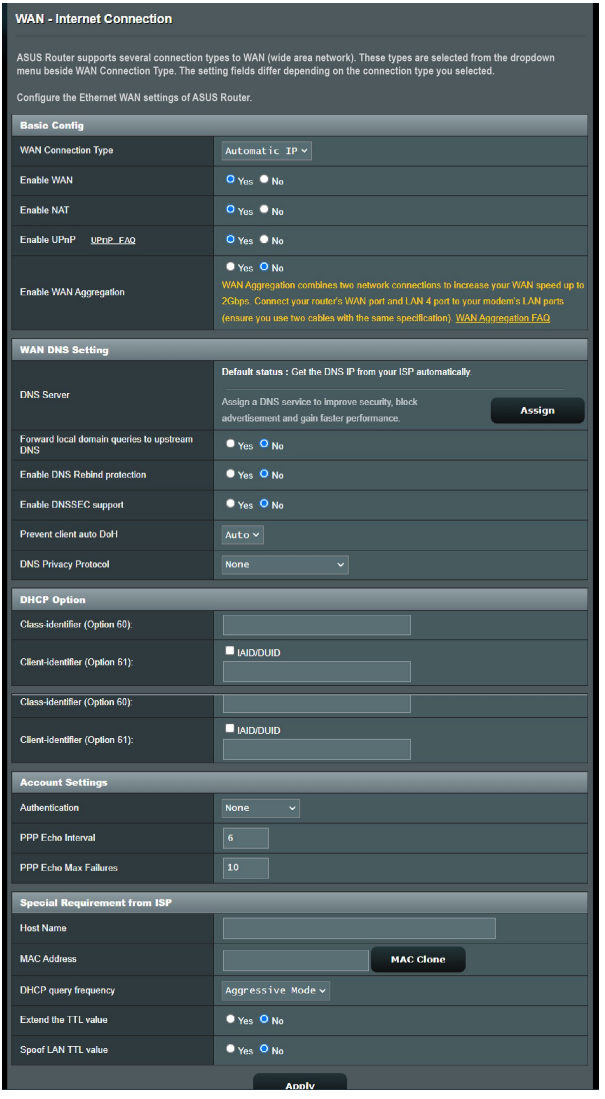
A função de monitorização de tráfego permite aceder à utilização da largura de banda e velocidade da ligação à Internet das suas redes com e sem fios. Permite-lhe monitorizar o tráfego da rede em tempo real ou por dia. Oferece também uma opção para exibir o tráfego de rede nas últimas 24 horas.

NOTA: Os pacotes da Internet são transmitidos uniformemente para os dispositivos com e sem fios.

3.11 WAN

3.11.1 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 **Advanced Settings (Definições avançadas)** > **WAN** > **Internet Connection (Ligação à Internet)**.
2. Configure as definições indicadas abaixo. Quando terminar, clique em **Apply (Aplicar)**.

- **WAN Connection Type (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 **fixed IP (IP fixo)**. Consulte o seu ISP se o router não conseguir obter um endereço IP válido ou se tem dúvidas acerca do tipo de ligação WAN.
- **Enable WAN** (**Ativar WAN)**: S.eleccione **Yes (Sim)** para permitir que o router aceda à Internet. Selecione **No (Não)** para desativar o acesso à Internet.
- **Enable NAT (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.
- **Enable UPnP (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.

- **Enable WAN Aggregation (Ativar Agregação de WAN):** WAN Aggregation (Agregação de WAN) combina duas ligações de rede para aumentar a velocidade da ligação WAN até 2 Gbps. Ligue a porta WAN do router e a porta LAN 4 às portas LAN do seu modem.
- **Connect to DNS Server (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.
- **Authentication (Autenticação)**: Este item poderá ser especificado por alguns ISPs. Consulte o seu ISP e preencha os dados, caso seja necessário.
- **Host Name (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.
- **MAC Address (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 sem fios ASUS para coincidir com o endereço MAC do dispositivo original reconhecido pelo ISP.

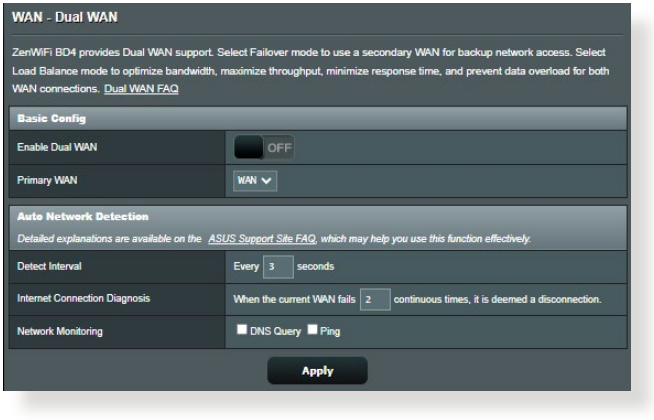
3.11.2 Dual WAN (WAN dupla)

A Dual WAN (WAN dupla) permite selecionar duas ligações de ISP para o seu router, uma WAN principal e uma WAN secundária.

Para configurar a Dual WAN (WAN dupla):

1. No painel de navegação, aceda a **Advanced Settings (Definições avançadas) > WAN**.
2. Aceda ao campo **Dual WAN (WAN dupla)** e defina para **ON (Ativado)**.
3. Escolha a **Primary WAN (WAN principal)** e **Secondary WAN (WAN secundária)**. Estão disponíveis duas opções de WAN/LAN 2.5GbE para sua escolha.
4. Escolha **Fail Over (Ativação pós-falha)** ou **Load Balance (Balanceamento de carga)**.
5. Clique em **Apply (Aplicar).**

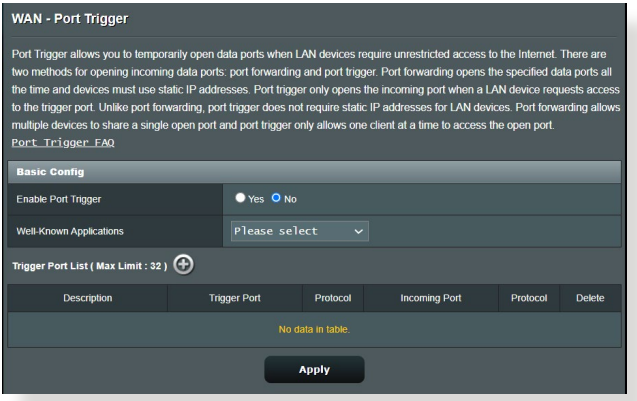
NOTA: Estão disponíveis explicações detalhadas na secção de perguntas frequentes do site de Suporte da ASUS **https://www.asus.com/support/FAQ/1011719**.



3.11.3 Ativação de Portas

A ativação de intervalos de portas abre uma porta de entrada predeterminada durante um período de tempo limitado sempre que um cliente da rede de área local efetua uma ligação de saída a uma porta específica. A ativação de portas é utilizada nas seguintes situações:

- Mais do que um cliente local precisa de reencaminhamento de portas para a mesma aplicação num momento diferente.
- Uma aplicação precisa de portas de entrada específicas que são diferentes das portas de saída.



Para configurar a Activação de Portas:

1. No painel de navegação, aceda a **Advanced Settings (Definições avançadas)** > **WAN** > **Port Trigger (Activação de Portas)**.
2. Configure as definições indicadas abaixo. Quando terminar, clique em **Apply (Aplicar)**.
   - **Enable Port Trigger (Ativar Ativação de Portas)**: Escolha **Yes (Sim)** para Ativar a Ativação de Portas.
   - **Well-Known Applications (Aplicações conhecidas)**: Selecione jogos e serviços Web populares para adicionar à Lista de Ativação de Portas.
   - **Description (Descrição)**: Introduza um nome abreviado ou uma descrição para o serviço.

- **Trigger Port (Porta de ativação)**: Especifique uma porta de activação para abrir a porta de entrada.
- **Protocol (Protocolo)**: Selecione o tipo de protocolo, TCP ou UDP.
- **Incoming Port (Porta de entrada)**: Especifique uma porta de entrada para receber dados da Internet.

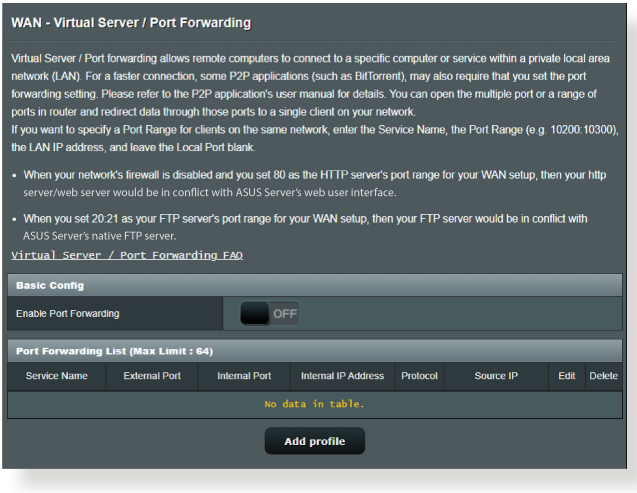
NOTAS:

- 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.

3.11.4 Servidor virtual/Reencaminhamento de portas

O reencaminhamento de chamadas é um método para direcionar tráfego de rede da Internet para uma porta específica ou um intervalo de portas para um ou vários dispositivos na sua rede local. A configuração do Reencaminhamento de Portas no seu router permite que PCs fora da rede tenham acesso a serviços específicos oferecidos por um PC na sua rede.

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 **Advanced Settings (Definições avançadas)** > **WAN** > **Virtual Server / Port Forwarding (Servidor virtual / Reencaminhamento de portas)**.
2. Configure as definições indicadas abaixo. Quando terminar, clique em **ON (Ativado)**.
   - **Enable Port Forwarding (Ativar reencaminhamento de portas)**: Defina para **ON (Ativado)** para ativar o Reencaminhamento de portas.

- **Famous Server List (Lista de servidores famosos)**: Escolha o tipo de serviço ao qual deseja aceder.
- **Famous Game List (Lista de jogos famosos)**: Este item apresenta a lista de portas necessárias para que jogos online populares funcionem corretamente.
- **FTP Server Port (Porta de servidor FTP)**: Evite definir o intervalo de portas 20:21 para o seu servidor FTP, pois irá causar conflito com o servidor FTP nativo do router.
- **Service Name (Nome do serviço)**: Introduza o nome do serviço.
- **Port Range (Intervalo de portas)**: Se deseja 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. O intervalo de portas aceita vários formatos como, por exemplo, Intervalos de portas (300:350), portas individuais (566, 789) ou Mistura (1015:1024, 3021).

NOTAS:

- Se a firewall da sua rede estiver desativada e a porta 80 for definir como porta do servidor HTTP na configuração da WAN, o seu servidor http/servidor Web estará em conflito com a interface Web do router.
- Uma rede utiliza as portas para transferir dados e cada porta tem um número atribuído e uma tarefa específica. Por exemplo, a porta 80 é utilizada para HTTP. Uma porta específica pode ser utilizada por uma aplicação ou serviço de cada vez. Por conseguinte, dois PCs que tentem aceder a dados em simultâneo através da mesma porta irão falhar. Por exemplo, não é possível configurar o Reencaminhamento de Portas para a porta 100 para dois PCs em simultâneo.

- **Local IP (IP Local)**: Introduza o endereço IP da LAN do cliente.

NOTA: Utilize um endereço IP estático para o cliente local para que o reencaminhamento de portas funcione corretamente. Para mais informações, consulte a secção **3.8 LAN**.

- **Local Port (Porta Local):** 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.
- **Protocol (Protocolo)**: Selecione o protocolo. Se tiver dúvidas, selecione **BOTH (AMBOS)**.

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.

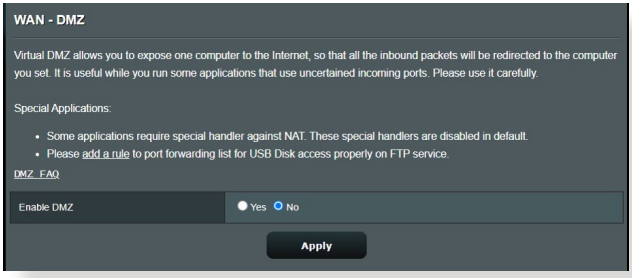
3.11.5 DMZ

O serviço DMZ Virtual expõe um cliente à Internet, permitindo que esse cliente receba todos os pacotes direcionados à sua rede de área local.

O tráfego recebido da Internet é geralmente rejeitado e encaminhado para um cliente específico apenas se o reencaminhamento de portas ou ativação de portas estiver configurado na rede. Numa configuração DMZ, um cliente da rede recebe todos os pacotes de entrada.

A configuração de DMZ numa rede é útil quando é necessário que as portas de entrada estejam abertas ou quando deseja alojar um servidor de domínio, Web ou de e-mail.

ATENÇÃO: A abertura de todas as portas num cliente para a Internet torna a rede vulnerável a ataques a partir do exterior. Tenha atenção aos riscos de segurança que envolvem a utilização de DMZ.



Para configurar o serviço DMZ:

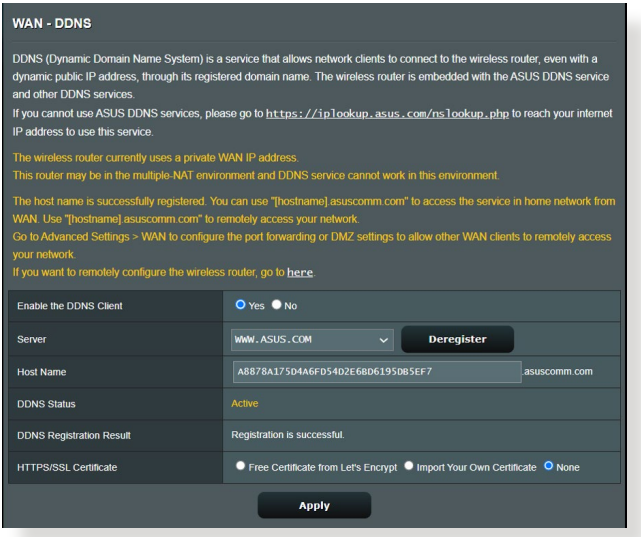
1. No painel de navegação, aceda a **Advanced Settings (Definições avançadas)** > **WAN** > **DMZ**.
2. Configure as definições indicadas abaixo. Quando terminar, clique em **Apply (Aplicar)**.
   - **IP address of Exposed Station (Endereço IP da estação exposta):** Introduza o endereço IP da LAN do 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)**.

3.11.6 DDNS

A configuração de DDNS (Dynamic DNS) permite-lhe aceder ao router a partir do exterior da sua rede através do Serviço ASUS DDNS ou outro serviço DDNS.



Para configurar o DDNS:

1. No painel de navegação, aceda a **Advanced Settings (Definições avançadas)** > **WAN** > **DDNS**.
2. Configure as definições indicadas abaixo. Quando terminar, clique em **Apply (Aplicar)**.
   - **Enable the DDNS Client (Ativar o cliente DDNS)**: Active o DDNS para aceder ao router ASUS através do nome DNS em vez do endereço IP da WAN.
   - **Server and Host Name (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).
- **Enable wildcard (Ativar caracteres universais)**: Ative os caracteres universais se o seu serviço DDNS o exigir.

NOTAS:

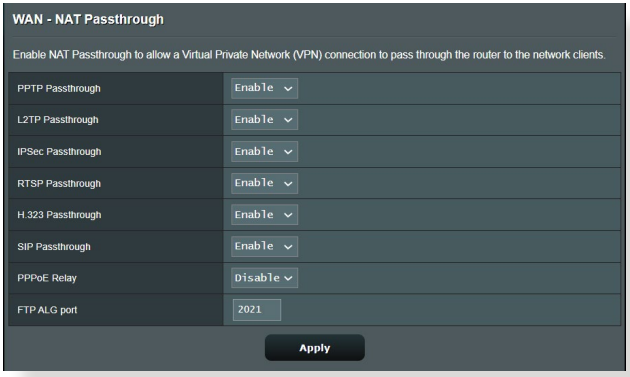
O serviço DDNS não funcionará nas seguintes condições:

- Quando o router sem 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.

3.11.7 Passagem de NAT

A Passagem de NAT permite que uma ligação de Rede Privada Virtual (VPN) passe pelo router para os clientes da rede. As definições Passagem de PPTP, Passagem de L2TP, Passagem de IPsec e Passagem de RTSP estão ativadas por predefinição.

Para Ativar/desativar as definições de Passagem de NAT, aceda a **Advanced Settings (Definições avançadas)** > **WAN** > **NAT Passthrough (Passagem de NAT)**. Quando terminar, clique em **Apply (Aplicar)**.

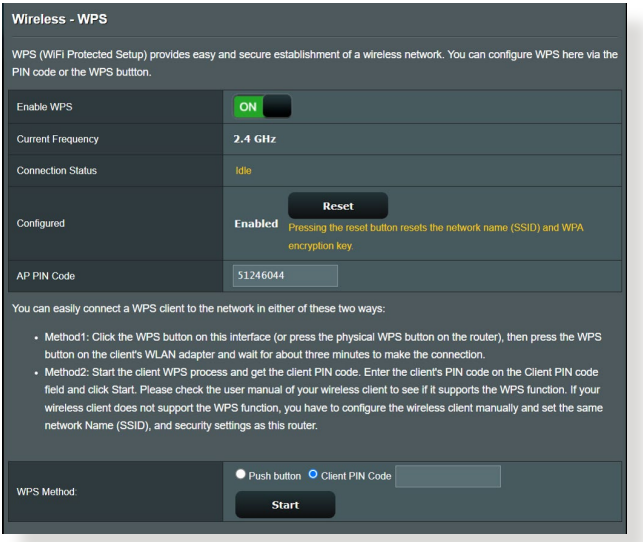


3.12 Sem fios

3.12.1 WPS

WPS (Configuração Wi-Fi Protegida) é uma norma de segurança sem fios que permite ligar facilmente dispositivos a uma rede sem fios. Pode configurar a função WPS através do código PIN ou do botão WPS.

NOTA: Certifique-se de que o dispositivo suporta a função WPS.



Para Ativar a função WPS no seu router sem fios:

1. No painel de navegação, aceda a **Advanced Settings (Definições avançadas)** > **Wireless (Sem fios)** > **WPS**.
2. No campo **Enable WPS (Ativar WPS)**, desloque o interruptor para a posição **ON (Ativado)**.
3. Poe predefinição, a função WPS utiliza a frequência de 2,4GHz. Se pretender mudar para a frequência de 5GHz, coloque o interruptor da função WPS na posição **OFF (Desativado)**, clique em **Switch Frequency (Mudar frequência)** no campo **Current Frequency (Frequência actual)** e coloque o interruptor da função WPS novamente na posição **ON (Ativado)**.

NOTA: A função WPS suporta os métodos de autenticação Sistema aberto, WPA-Pessoal e WPA2-Pessoal. A função WPS não suporta redes sem fios que utilizem os métodos de encriptação Chave partilhada, WPA-Empresarial, WPA2-Empresarial e RADIUS.

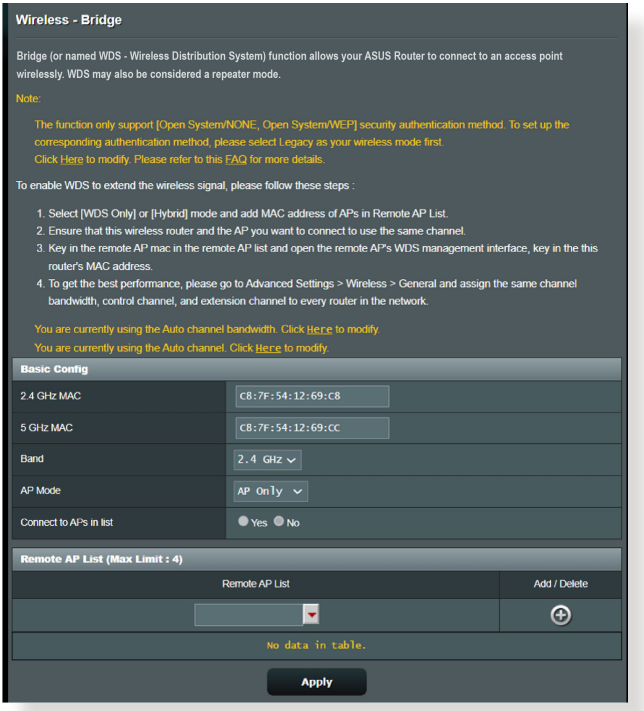
4. No campo WPS Method (Método de WPS), Selecione **Push Button (Botão)** ou o **Client PIN Code (Código PIN do cliente)**. Se seleccionar **Push Button (Botão)**, avance para o passo 5. Se seleccionar o **Client PIN Code (Código PIN do cliente)**, avance para o passo 6.
5. Para configurar a função WPS utilizando o botão WPS do router, siga estes passos:
   a. Clique em **Start (Iniciar)** ou pressione o botão WPS existente na parte posterior do router sem fios.
   b. Pressione o botão WPS no seu dispositivo sem fios. Esse botão está geralmente identificado com o logótipo WPS.

   NOTA: Verifique o seu dispositivo ou o respectivo manual para saber a localização do botão WPS.

   c. O router sem fios irá procurar todos os dispositivos WPS disponíveis. Se o router sem fios não encontrar dispositivos WPS, irá mudar para o modo normal.
6. Para configurar a função WPS utilizando o código PIN do cliente, siga estes passos:
   a. Localize o código PIN WPS no manual do utilizador do seu dispositivo sem fios ou no próprio dispositivo.
   b. Introduza o código PIN do cliente na caixa de texto.
   c. Clique em **Start (Iniciar)** para colocar o router sem fios no modo de pesquisa WPS. Os indicadores LED do router irão piscar rapidamente três vezes até que a configuração de WPS esteja concluída.

3.12.2 Bridge

A função Bridge ou WDS (Sistema de Distribuição Sem Fios) permite que o seu router sem fios ASUS se ligue exclusivamente a outro ponto de acesso sem fios, impedindo que outros dispositivos ou estações sem fios acedam ao seu router sem fios ASUS. Pode também ser considerado um repetidor de sinal sem fios onde o seu router sem fios ASUS comunica com outro ponto de acesso e outros dispositivos sem fios.



Para configurar a função Bridge rede sem fios:

1. No painel de navegação, aceda a **Advanced Settings (Definições avançadas)** > **Wireless (Sem fios)** > **WDS**.
2. Selecione a banda de frequência para a Bridge sem fios.
3. No campo **AP Mode (Modo AP)**, Selecione uma destas opções:
   - **AP Only (Apenas AP)**: Desativa a função Bridge sem fios.
   - **WDS Only (Apenas WDS)**: Ativa a função Bridge sem fios mas impede que outros dispositivos/estações se liguem ao router.

- **HYBRID (HÍBRIDO)**: Ativa a função Bridge sem fios mas permite que outros dispositivos/estações se liguem ao router.

NOTA: No modo Híbrido, os dispositivos sem fios ligados ao router sem fios ASUS receberão apenas metade da velocidade de ligação do Ponto de Acesso.

4. No campo **Connect to APs in list (Ligar a APs na lista)**, clique em **Yes (Sim)** se deseja ligar a um Ponto de Acesso da Lista de AP Remotos.
5. No campo **Control Channel (Canal de controlo)**, Selecione o canal de funcionamento para a Bridge sem fios. Selecione **Auto** para permitir que o router Selecione automaticamente o canal com menor interferência.

NOTA: A disponibilidade dos canais varia de acordo com o país ou região.

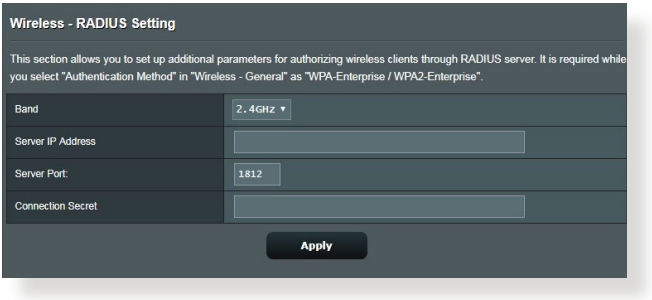
6. Na **Remote AP List (Lista de AP Remotos)**, introduza um endereço MAC e clique no botão **Add (Adicionar)**  para introduzir o endereço MAC de outros Pontos de Acesso disponíveis.

NOTA: Os Pontos de Acesso adicionados à lista deverão estar no mesmo Canal de Controlo do router sem fios ASUS.

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

3.12.3 Configuração de RADIUS

A Configuração de RADIUS (Remote Authentication Dial In User Service) oferece um nível adicional de segurança quando escolher WPA-Empresarial, WPA2-Empresarial ou Radius com 802.1x como Modo de Autenticação.



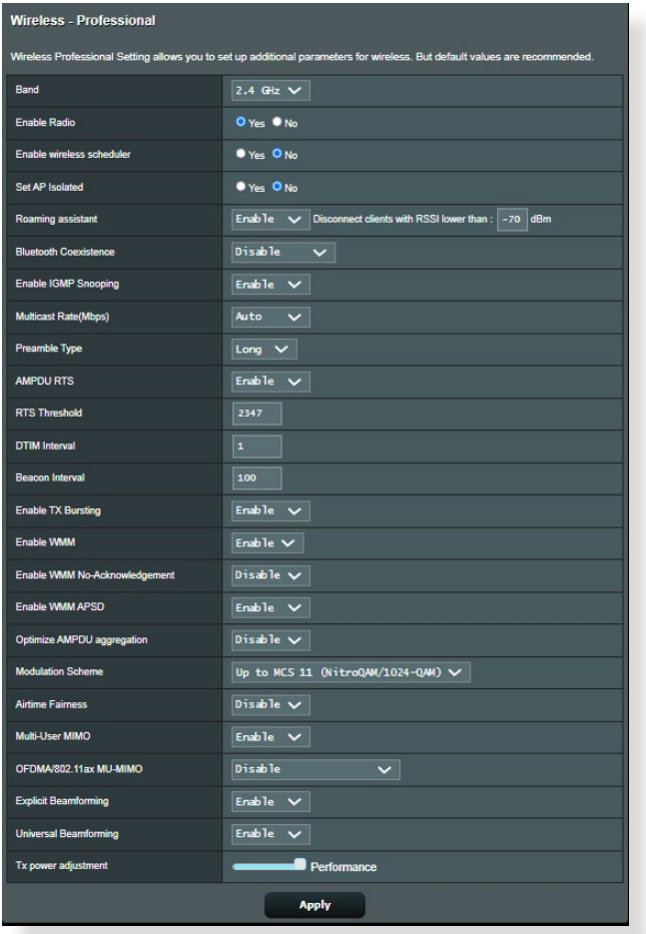
Para configurar as definições de RADIUS sem fios:

1. Certifique-se de que o modo de autenticação do router sem fios está definido como WPA-Empresarial, WPA2-Empresarial ou Radius com 802.1x.
2. No painel de navegação, aceda a **Advanced Settings (Definições avançadas)** > **Wireless (Sem fios)** > separador **RADIUS Setting (Configuração de RADIUS)**.
3. Selecione a banda de frequência.
4. No campo **Server IP Address (Endereço IP do servidor)**, introduza o endereço IP do servidor RADIUS.
5. No campo **Connection Secret (Segredo de ligação)**, defina a palavra-passe para aceder ao servidor RADIUS.
6. Clique em **Apply (Aplicar)**.

3.12.4 Profissional

O ecrã Professional (Profissional) disponibiliza opções de configuração avançadas.

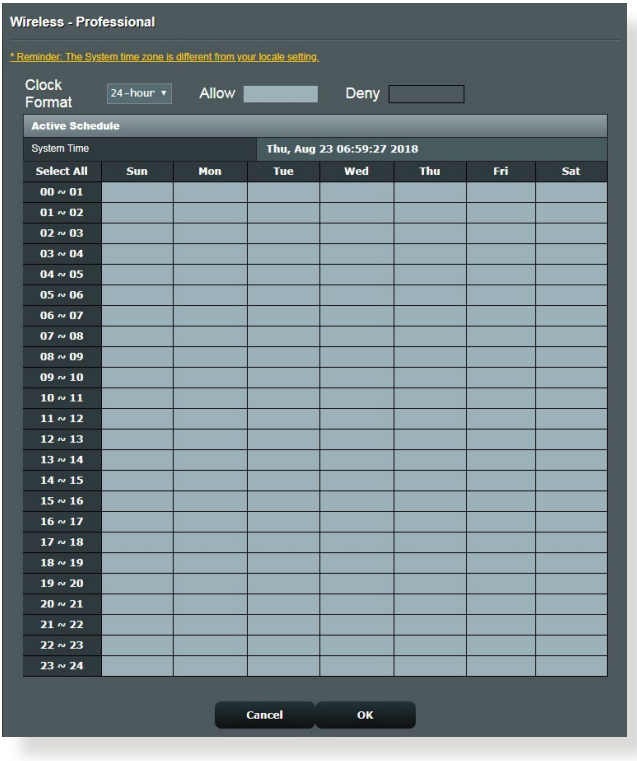
NOTA: Recomendamos que utilize os valores predefinidos nesta página.



No ecrã **Professional Settings (Definições profissionais)**, pode configurar as seguintes definições:

- **Band (Banda)**: Selecione a banda de frequência à qual serão aplicadas as definições profissionais.

- **Enable Radio (Ativar rádio)**: Selecione **Yes (Sim)** para Ativar a rede sem fios. Selecione **No (Não)** para desativar a rede sem fios.
- **Enable wireless scheduler (Ativar agenda sem fios):** Pode escolher o formato de relógio de 24 ou 12 horas. As cores na tabela indicam Permitir ou Recusar. Clique em cada célula para alterar as definições da hora dos dias da semana e clique em **OK** quando terminar.



- **Set AP isolated (Definir AP isolado)**: O item Set AP isolated (Definir IP isolado) impede que os dispositivos sem fios da sua rede comuniquem entre si. Esta função é útil se muitos convidados aderirem ou abandonarem frequentemente a sua rede. Selecione **Yes (Sim)** para Ativar esta função ou selecione **No (Não)** para desativar.
- **Multicast rate (Mbps) (Velocidade Multicast (Mbps))**: Selecione a velocidade de transmissão de multicast ou clique em **Disable (Desativar)** para desativar a transmissão simultânea.

- **Preamble Type (Tipo de preâmbulo)**: O tipo de preâmbulo define o tempo gasto pelo router para CRC (Controlo de Redundância Cíclica). CRC é um método para detectar erros durante a transmissão de dados. Selecione **Short (Curto)** para uma rede sem fios com tráfego de rede elevado. Selecione **Long (Longo)** se a sua rede sem fios é composta por dispositivos sem fios antigos.
- **RTS Threshold (Limite de RTS)**: Selecione um valor mais baixo para o Limite de RTS (Pedido de Envio) para melhorar a comunicação sem fios na rede com tráfego elevado e diversos dispositivos sem fios.
- **DTIM Interval (Intervalo de DTIM)**: O Intervalo de DTIM (Delivery Traffic Indication Message) ou Velocidade de Sinalização de Dados é o intervalo de tempo antes do envio de um sinal para um dispositivo sem fios em modo de suspensão, indicando que um pacote de dados está a aguardar entrega. O valor predefinido é três milissegundos.
- **Beacon Interval (Intervalo de sinalização)**: O Intervalo de sinalização é o tempo entre um DTIM e o seguinte. O valor predefinido é 100 milissegundos. Diminua o valor do Intervalo de sinalização para uma ligação sem fios instável ou para dispositivos em roaming.
- **Enable TX Bursting (Ativar rajada de transmissão)**: A função Ativar rajada de transmissão melhora a velocidade de transmissão entre o router sem fios e dispositivos 802.11g.
- **Enable WMM APSD (Ativar WMM APSD)**: Active a função WMM APSD (Wi-Fi Multimedia Automatic Power Save Delivery) para melhorar a gestão de energia entre dispositivos sem fios. Selecione **Disable (Desativar)** para desativar a função WMM APSD.

4 Utilitários

4.1 O Deteção de dispositivos

O Deteção de dispositivos é um utilitário para a WLAN da ASUS que detecta o router sem fios da ASUS e permite-lhe configurar as definições da rede sem fios.

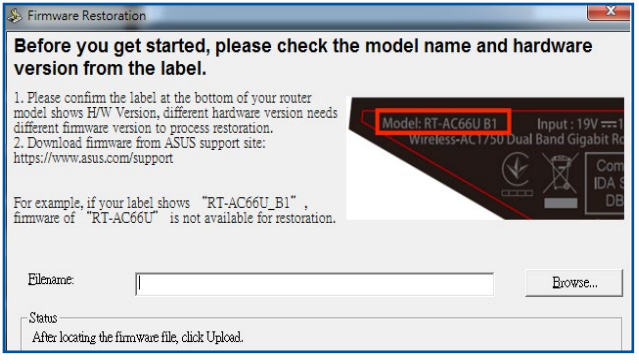
Para abrir o Deteção de dispositivos:

- No ambiente de trabalho do computador, clique em **Start (Iniciar) > All Programs (Todos os programas) > ASUS Utility (Utilitário da ASUS) > Router sem fios ASUS > Device Discovery (Deteção de dispositivos)**.

NOTA: Quando utilizar o router no modo de Ponto de Acesso, deverá utilizar a Descoberta de Dispositivos para obter o endereço IP do router.

4.2 O Restauro do Firmware

O utilitário Firmware Restoration (Restauro do Firmware) é utilizado num Router Sem Fios ASUS que falhou durante o processo de atualização do firmware. Este utilitário atualiza o firmware especificado pelo utilizador. O processo demora cerca de três a quatro minutos.



IMPORTANTE! Inicie o modo de recuperação antes de utilizar o utilitário Firmware Restoration (Restauro do Firmware).

NOTA: Esta funcionalidade não é suportada no MAC OS.

Para lançar iniciar o modo de recuperação e usar o utilitário Firmware Restoration (Restauro do Firmware):

1. Desligue o router sem fios da corrente eléctrica.
2. Mantenha premido o botão de reposição no painel traseiro e em simultâneo volte a ligar o router sem fios à corrente eléctrica. Liberte o botão de reposição quando o LED de Alimentação no painel frontal piscar lentamente, o que indica que o router sem fios se encontra no modo de recuperação.
3. Configure um IP estático no seu computador e utilize as seguintes informações para configurar as definições de TCP/IP:

   IP address (Endereço IP): 192.168.1.x

   Subnet mask (Máscara de sub-rede): 255.255.255.0
4. No ambiente de trabalho do seu computador, clique em **Start (Iniciar) > All Programs (Todos os programas) > ASUS Utility (Utilitário ASUS) > Wireless Router (Router sem fios) > Firmware Restoration (Restauro do Firmware)**.
5. Especifique um ficheiro de firmware, depois clique em **Upload (Enviar)**.

NOTA: Este não é um utilitário para atualização de firmware e não pode ser utilizado num Router ASUS que esteja a funcionar corretamente. As atualizações normais do firmware devem ser realizadas através da interface da Web. Consulte o **Capítulo 3: Configurar as definições gerais e avançadas** para mais detalhes.

5 Resolução de problemas

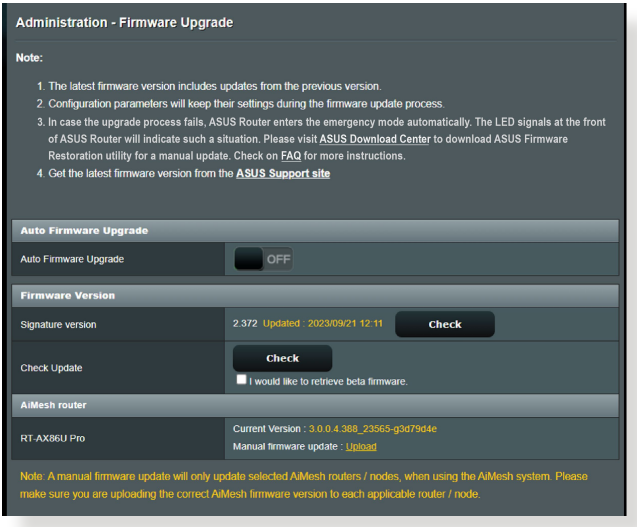
Este capítulo apresenta soluções para problemas que poderão ocorrer no seu router. Se ocorrerem problemas não mencionados neste capítulo, visite o site de apoio da ASUS em: https://www.asus.com/support para obter mais informações sobre o produto e detalhes de contacto da Assistência Técnica da ASUS.

5.1 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 **Advanced Settings (Definições avançadas)** > **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 em https://www.asus.com/Networking/ZenWiFi BD4/HelpDesk/ para transferir o firmware mais recente.

3. Na página **Firmware Version (Versão de firmware)**, clique em **Check (Verificar)** 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 a configuração da rede sem fios do computador coincide com a do seu router.

- Quando ligar o seu computador ao router através de ligação sem fios, certifique-se de que o SSID (nome da rede sem fios), o método de encriptação e a palavra-passe estão corretos.

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 sem 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, **Network Map (Mapa de Rede)** > **Clients (Clientes)**, colocando o ponteiro do rato sobre o dispositivo na secção **Client status (Estado do cliente)**.

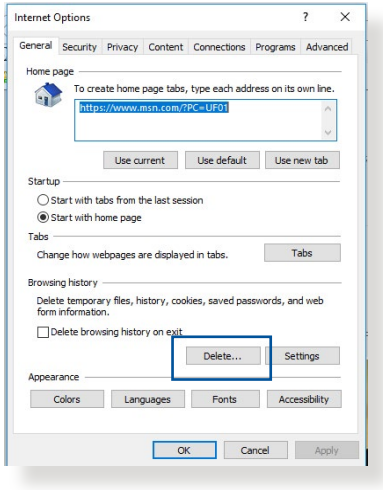
5.2 Perguntas Frequentes (FAQs)

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)**.



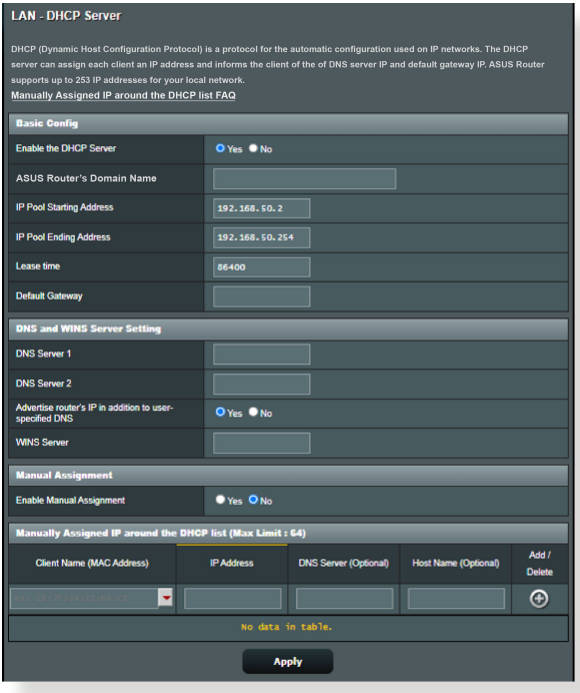
NOTAS:

- 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.

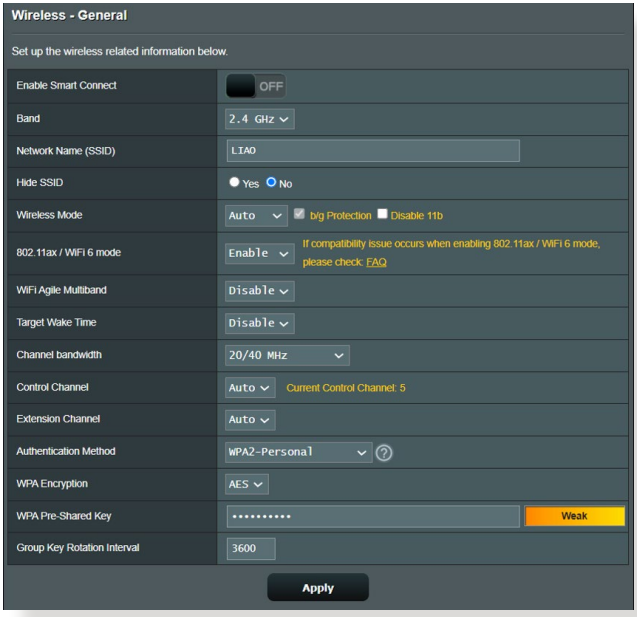
O cliente não consegue estabelecer uma ligação sem fios com o router.

NOTA: Se não conseguir ligar a uma rede de 5GHz, certifique-se de que o seu dispositivo sem fios suporta a banda 5GHz ou tem capacidades de duas bandas.

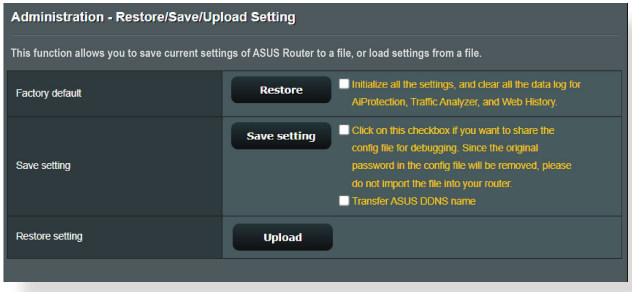
- **Fora de alcance:**
  - Coloque o router mais próximo do cliente sem fios.
- **O servidor DHCP foi desativado:**
  1. Aceda à Interface Web do utilizador. Aceda a **General (Geral)** > **Network Map (Mapa de Rede)**> **Clients (Clientes)** e procure dispositivos que deseja ligar ao router.
  2. Se não conseguir encontrar o dispositivo no **Network Map (Mapa de Rede)**, aceda a **Advanced Settings (Definições avançadas)** > **LAN** > **DHCP Server (Servidor DHCP)**, lista **Basic Config (Configuração básica)**, selecione **Yes (Sim)** no campo **Enable the DHCP Server (Ativar o 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 **Advanced Settings (Definições avançadas)** > **Wireless (Sem fios)** > **General (Geral)**, selecione **No (Não)** no campo **Hide SSID (Ocultar SSID)** e selecione **Auto** no campo **Control Channel (Canal de controlo)**.



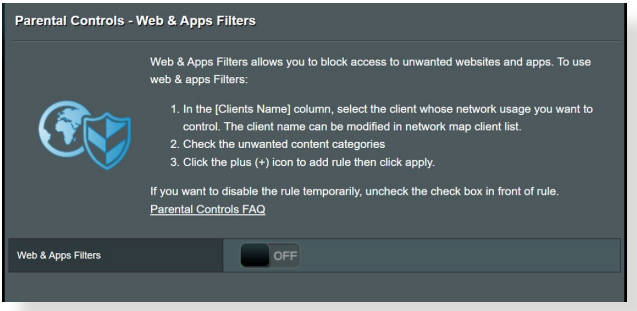
- Se estiver a utilizador um adaptador de LAN sem fios, verifique se o canal sem fios em utilização está em conformidade com os canais disponíveis no seu país/área. Caso contrário, ajuste o canal, a largura de banda do canal e o modo sem fios.
- Se mesmo assim não conseguir ligar ao router, pode repor as predefinições do router. Na interface de utilizador do router, clique em **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 **General (Geral)** > **Network Map (Mapa de Rede)** e verifique o **Internet Status (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)**.

- O dispositivo foi bloqueado através da função de Controlo Parental. Aceda a **General (Geral) > Parental Controls (Controlo Parental)** e verifique se o dispositivo está na lista. Se o dispositivo estiver na lista **Client Name (Nome do cliente)**, remova o dispositivo utilizando o botão **Delete (Eliminar)** ou ajuste as Definições de Gestão de Tempo.



- Se mesmo assim não tiver acesso à Internet, experimente reiniciar o seu computador e verifique o endereço IP e gateway da rede.

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 **Network Map (Mapa de Rede)**, 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 **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 **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. Consulte a secção **4.2 Restauro do firmware** para saber como utilizar o utilitário de Restauro do firmware.

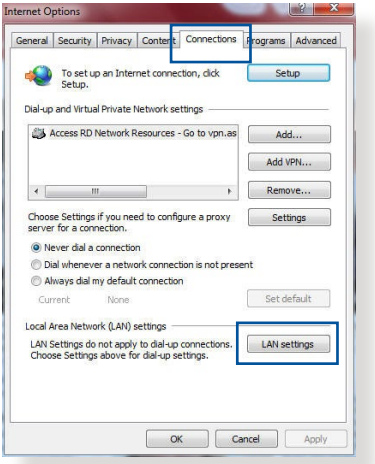
Não é possível aceder à Interface Web

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

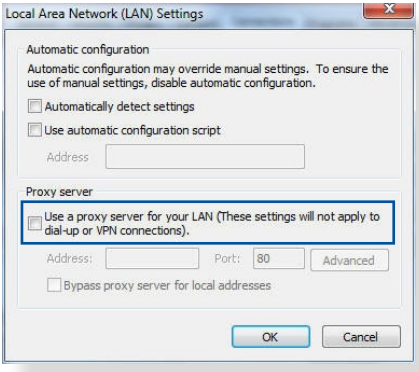
A. Desative o servidor proxy, caso esteja ativado.

Windows®

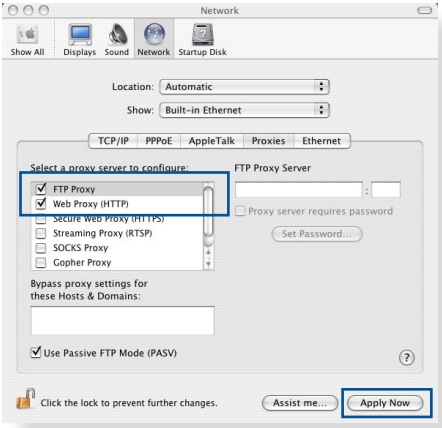
1. Clique em **Start (Iniciar)** > **Internet Explorer** para executar o navegador Web.
2. Clique em **Tools (Ferramentas) > Internet options (Opções da Internet) > Connections (Ligações) > LAN settings (Definições de LAN)**.



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



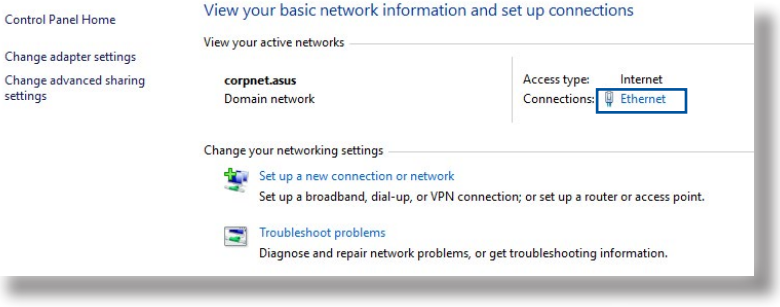
1. No navegador Safari, clique em **Safari > Preferences (Preferências) > Advanced (Avançadas) > Change Settings... (Alterar definições…)**.
2. No ecrã Network (Rede), desmarque **FTP Proxy** e **Web Proxy (Proxy Web) (HTTP)**.
3. Clique em **Apply Now (Aplicar agora)** quando terminar.

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

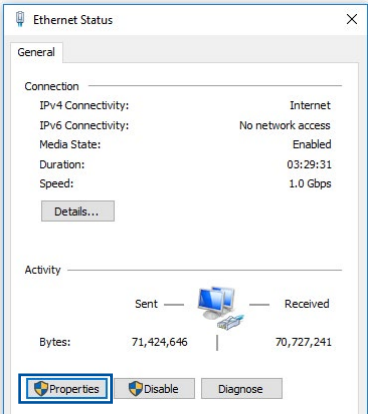
B. Configurar as definições de TCP/IP para obter automaticamente um endereço IP.

Windows®

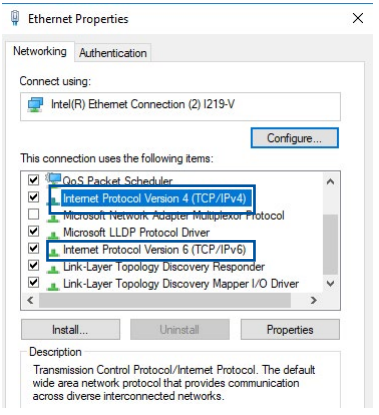
1. Clique em **Start (Iniciar) > Control Panel (Painel de Controlo) > Network and Sharing Center (Centro de Rede e Partilha)**, em seguida, clique na ligação de rede para exibir a janela de estado.



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



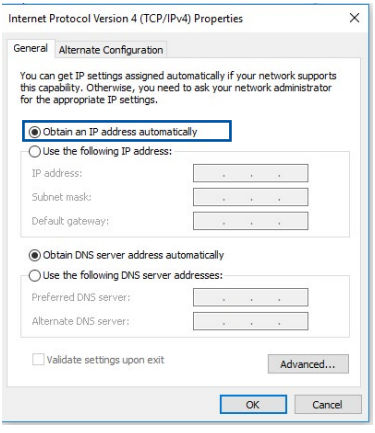
3. Selecione **Internet Protocol Version 4 (TCP/IPv4) (Internet Protocol Versão 4 (TCP/IPv4))** ou **Internet Protocol Version 6 (TCP/IPv6) (Internet Protocol Versão 6 (TCP/IPv6))** depois clique em **Properties (Propriedades)**.



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

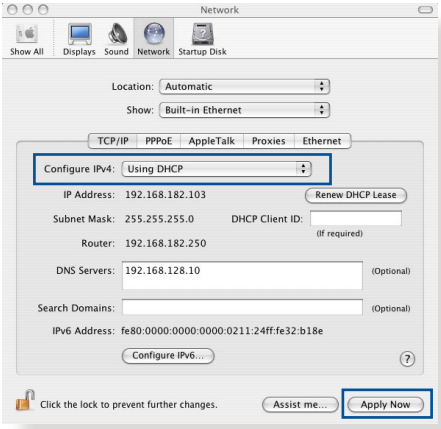
   Para configurar automaticamente as definições de iPv6 IP, marque a opção **Obtain an IPv6 address automatically (Obter automaticamente um endereço IPv6)**.

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)**.



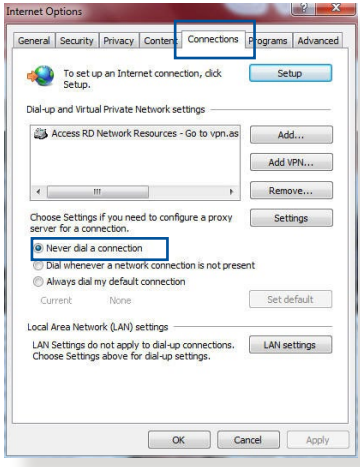
4. Clique em **Apply Now (Aplicar agora)** quando terminar.

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.