Manual de usuário

HG100R-L4

Aviso

Obrigado por adquirir um produto HUMAX. Por favor, leia este manual do usuário com atenção para poder instalar, usar e fazer manutenção do produto no desempenho máximo e com segurança. Mantenha este manual do usuário próximo de seu produto para futura consulta. As informações contidas neste manual do usuário estão sujeitas a alterações sem aviso prévio.

Copyright (Copyright © 2015 HUMAX Corporation)

Informações de Segurança e Regulamentação

Instruções de Segurança

Por favor, leia estas instruções antes de utilizar o gateway residencial. Nós não queremos que você se machuque ou que seu gateway residencial fique danificado.

- Não utilize o seu gateway residencial perto da água. Mantenha o seu gateway residencial seco. Se você precisa limpá-lo, não use uma toalha molhada. Limpe o gateway residencial com um pano limpo e seco. Nunca use produtos químicos de limpeza ou fluidos semelhantes. Não borrife produtos de limpeza diretamente sobre o gateway residencial nem use ar comprimido para remover o pó.

- Não coloque o seu gateway residencial perto de fontes de calor, como aparelhos quentes, por exemplo, radiadores, aquecedores e outros aparelhos eletrônicos como computadores e aparelhos de som, ou dentro de sua lareira. O seu gateway residencial é frio, e você deve ajudá-lo a ficar dessa maneira.

- Não cubra o gateway residencial, ou bloqueie o fluxo de ar para o gateway com nenhum objeto. Mantenha o gateway residencial longe de calor e da umidade excessiva e mantenha o gateway residencial sem vibração e poeira.

- O gateway residencial é apenas para uso interno. Por favor, não tente usá-lo na parte externa.

- Não tente abrir, modificar ou reparar o seu gateway residencial. Isso pode causar choque elétrico ou lesão em você. Qualquer modificação feita pelo cliente não expressamente aprovada pela HUMAX invalida a sua autoridade para operar o equipamento e anulará a garantia do gateway residencial.

- Ligue somente os cabos e acessórios especificados e conforme indicados pelo gateway da HUMAX.

- Proteja o cabo de alimentação do seu gateway residencial, permitindo-o que fique livremente entre o gateway residencial e a tomada. Não estique ou comprima-o entre os objetos.

- Manuseie seu gateway residencial com cuidado. Não deixe cair nem agite seu gateway residencial.

- É provável que seu gateway residencial irá aquecer, mas ele precisa de ventilação para continuar a funcionar corretamente. Não bloqueie as saídas de ar. É importante que o gateway seja colocado sobre uma superfície desobstruída e sólida. Não coloque o gateway em uma superfície macia, como um carpete, pois isso pode bloquear o fluxo de ar.

- O gateway residencial foi qualificado em condições de teste que incluíram a utilização dos cabos fornecidos entre sistemas componentes. Para garantir conformidade com regulamentação e segurança, use somente os cabos de alimentação e de interface fornecidos, e instale-os adequadamente.

- Adie a instalação até que não haja nenhum risco de trovoada ou relâmpagos na área.

- Evite utilizar o telefone (que não seja um tipo sem fio) durante uma tempestade elétrica. Pode existir um risco remoto de choque elétrico por causa de raios. Para aumentar ainda mais a proteção, desligue o gateway residencial da tomada da parede e desconecte os cabos para evitar danos a este gateway devido a raios e picos de energia.

- Após a conclusão de qualquer serviço ou reparação a este gateway residencial, peça ao técnico do serviço para executar verificações de segurança e determinar se o gateway residencial está em condições seguras de operação.

Riscos de asfixia

A embalagem do gateway residencial pode incluir sacos plásticos e braçadeiras. Descarte estes itens corretamente e mantenha-os fora do alcance de crianças, pois elas poderiam estar em risco de sofrer asfixia. Mantenha o gateway residencial, seus cabos e seus acessórios fora do alcance de crianças pequenas.

Acesso à página da WEB

Para configurar seu gateway residencial, você tem que acessar a página da web de configuração. O endereço IP do gateway residencial é 192.168.0.1. Para configurar o gateway residencial, siga as etapas abaixo:

1. Obtenha um endereço IP do servidor DHCP embutido para o PC para conectar o seu produto.

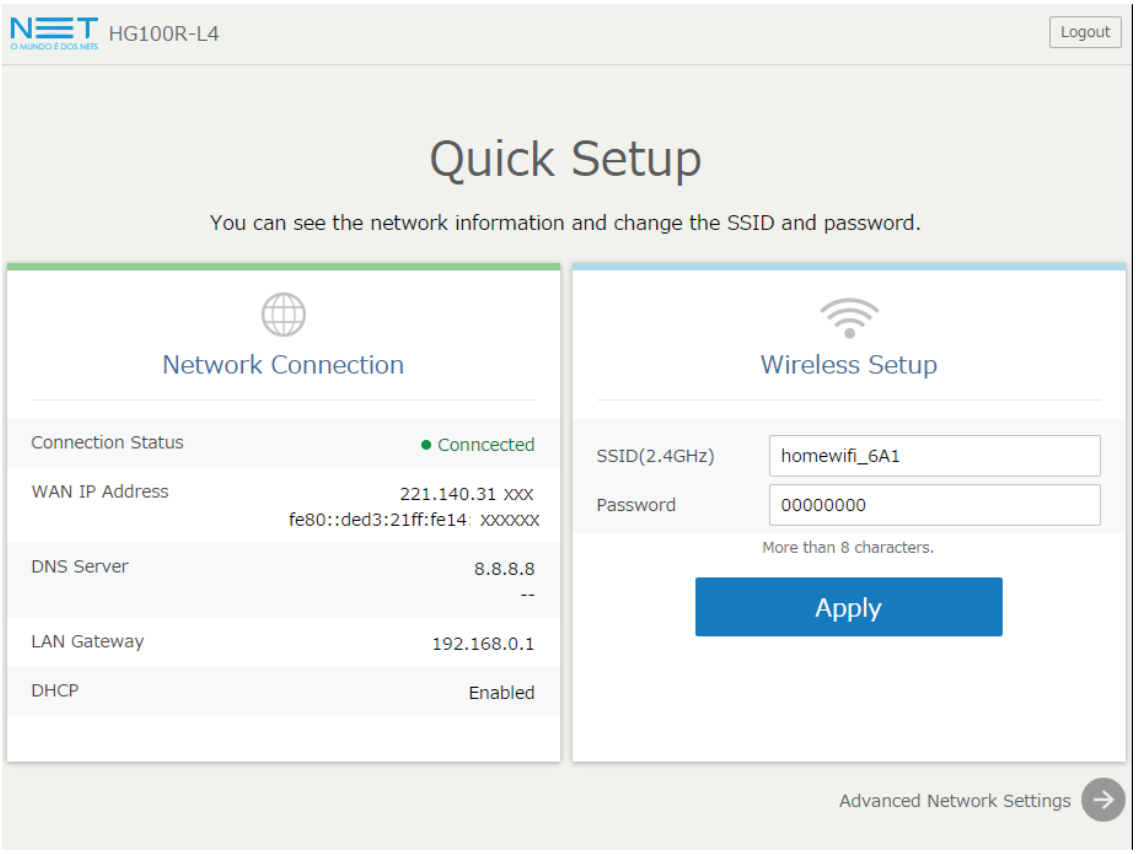
2. Abra o navegador da web (Internet Explorer, Chrome, Mozilla, etc.) no seu PC.

3. Digite **http://192.168.0.1** e a página de login é exibida. O ID padrão é **admin** e a senha é o endereço MAC do seu produto. O endereço MAC é descrito na parte inferior do produto.

Configurações rápidas

Você pode ver as informações de rede e alterar o SSID e a senha na página de configuração rápida. Basta inserir um novo SSID e senha e, em seguida, clique em Apply.

Para configurar seu gateway residencial em mais detalhes, selecione o ícone de seta. Em seguida, você é direcionado primeiro à página de status da conexão. Você pode voltar para a página de configuração rápida a qualquer momento, clicando em Quick Setup.

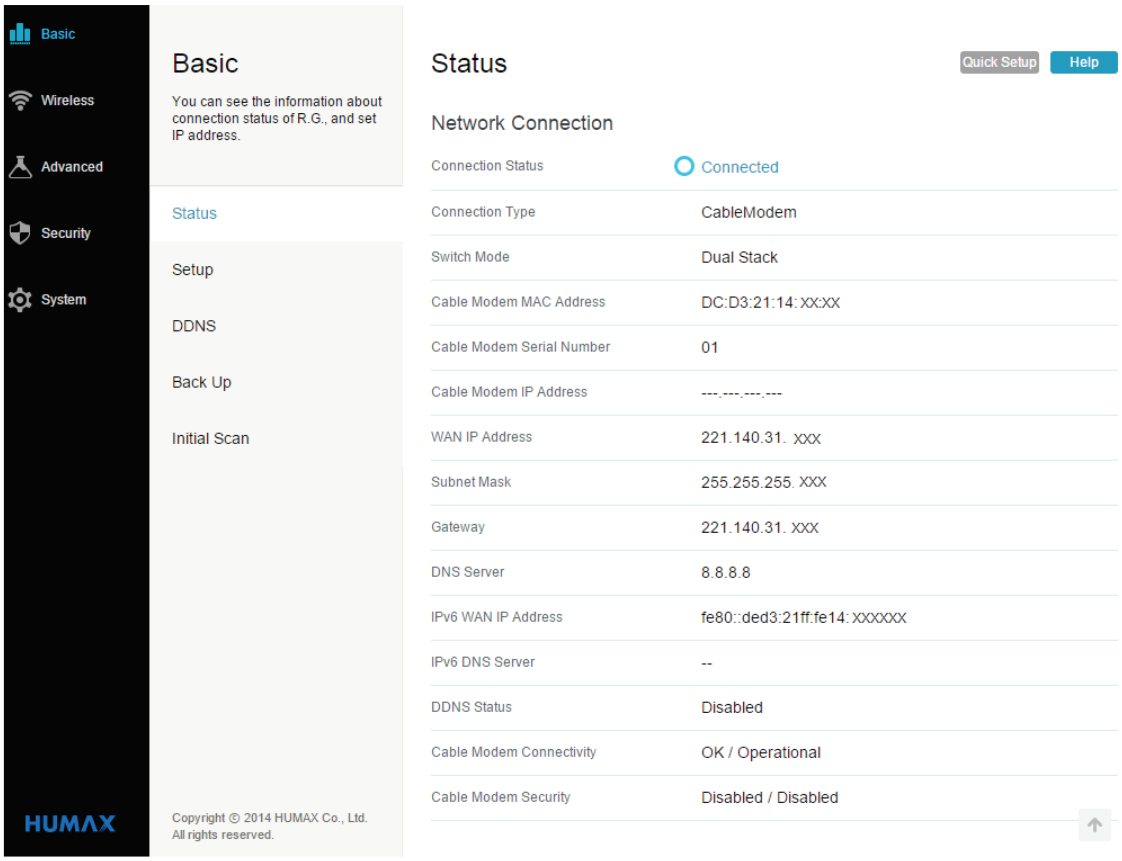


Informações de rede

Basic → Status

Você pode verificar as informações sobre o seu produto e a conectividade da rede.

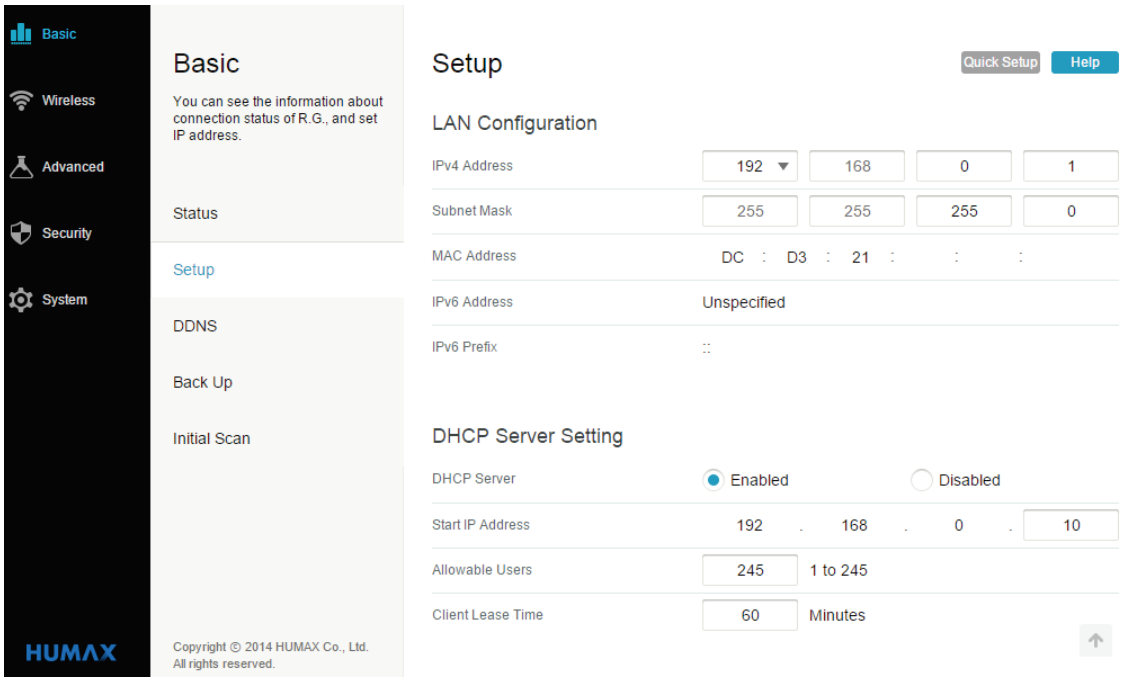
Nota: As informações desta página podem ser alteradas a qualquer momento, atualizando o seu navegador da web.



Configurações básicas

Basic → Status

Você pode configurar as funcionalidades básicas do gateway residencial e a conectividade da rede. Insira as informações necessárias nos campos para configurar seu gateway residencial.

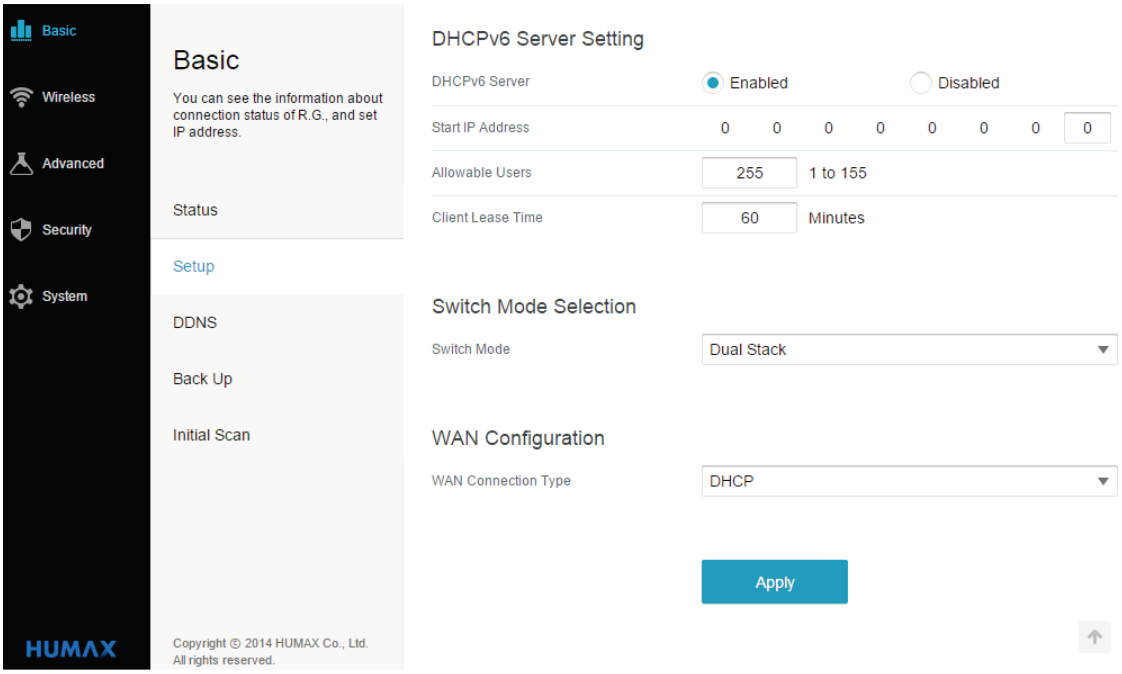


Configuração da LAN

- IPv4 Address: Digite o endereço IP do seu gateway residencial na sua LAN privada.
- Subnet Mask: Digite a máscara de sub-rede para a porta WAN.
- MAC Address: O endereço de controle de acesso de mídia é apresentado.
- IPv6 Address: Digite o endereço IPv6 do seu gateway residencial na sua LAN privada.
- IPv6 Prefix: Formato de comprimento do Endereço/Prefixo

Configuração do Servidor DHCP

- DHCP Server: Selecione Enabled para ativar o servidor de DHCP na sua LAN.
- Start IP Address: Insira o endereço IP inicial a ser atribuído pelo servidor DHCP para os clientes.
- Allowable Users: Introduza o número de clientes para o servidor DHCP a se atribuir um endereço IP privado.
- Client Lease Time: Digite a quantidade de tempo que o usuário receberá. Após esse tempo, o usuário será automaticamente atribuído a um novo endereço IP dinâmico.



Configuração do Servidor DHCPv6

- DHCPv6 Server: Selecione Enabled para ativar o servidor de DHCPv6 na sua LAN.
- Start IP Address: Insira o endereço IP inicial a ser atribuído pelo servidor DHCP para os clientes.
- Allowable Users: Insira o número de clientes para o servidor DHCP a se atribuir um endereço IP privado.
- Client Lease Time: Insira a quantia de tempo que o usuário será automaticamente atribuído um novo endereço IP dinâmico.

Seleção de Switch Mode

- Switch Mode: Selecione a opção.

  IPv4: Opera em modo NAT quando usando endereços IPv4

  IPv6: Opera em modo NAT quando usando endereços IPv6

  Dual Stack: Opera em modo NAT quando usando endereços IPv6 e IPv4

  Bridge: Opera em modo bridge

Configuração WAN

- WAN Connection Type: Selecione a opção.

  DHCP: Atribui endereços IP automaticamente para os dispositivos de cliente.

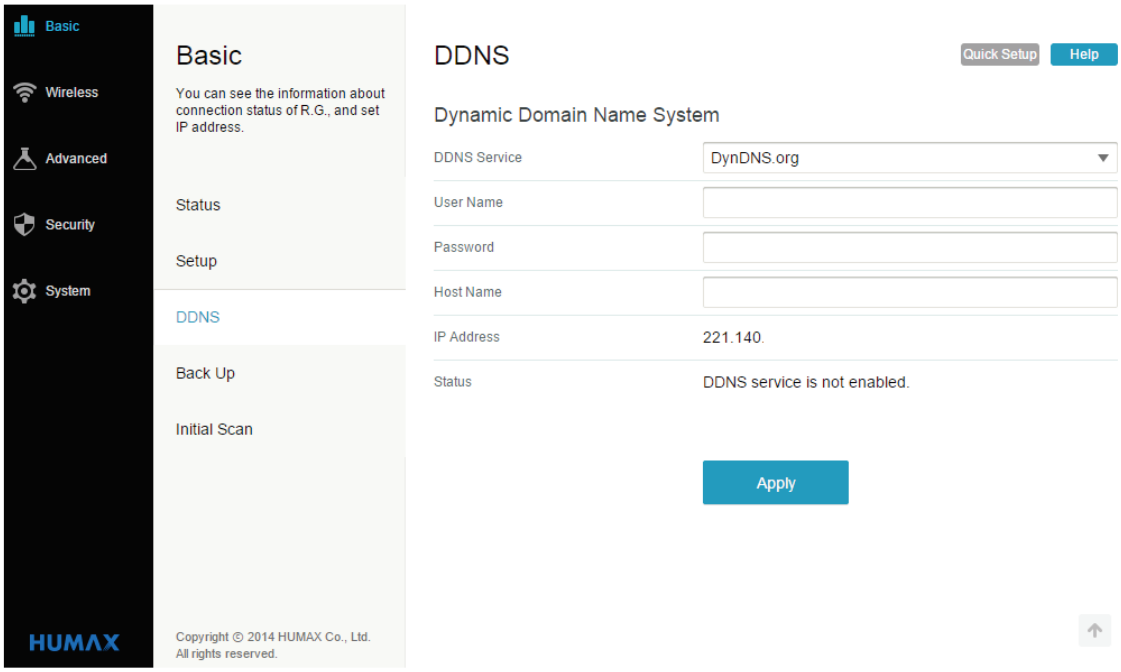
  Static IP: Insira o endereço IP, a máscara de sub-rede, gateway e DNS.

Suporte DNS Dinâmico

Basic → DDNS

Dynamic DNS (DDNS) permite que um endereço de IP dinâmico seja sinônimo de um nome de host estático e predefinido, para que o host possa ser facilmente contatado por outros hosts na Internet, mesmo que seu endereço IP mude.

O gateway residencial oferece suporte a um cliente DNS dinâmico compatível com o serviço Dynamic DNS ou No-IP.



Sistema de Nome de Domínio Dinâmico

Como ativar o cliente DDNS

1. Vá para http://www.dyndns.com ou http://www.noip.com e crie uma conta para o serviço Dynamic DNS.

- Efetue login no DynDNS ou No-IP com o nome de usuário e a senha.
- Vá para My Account > My Services > Add Host Services.
- Digite o nome do host para o seu servidor e selecione Dynamic DNS domain para atribuir o seu host.
- Verifique se o intervalo de repetição em que o gateway residencial tenta várias vezes entrar em contato com o servidor de nomes de domínio.
- Verifique o endereço IP atual de seu host. Este é o endereço IP da WAN que foi atribuído ao seu CMG durante o provisionamento. (Veja Endereço IP WAN em Basic/Setup menu.)

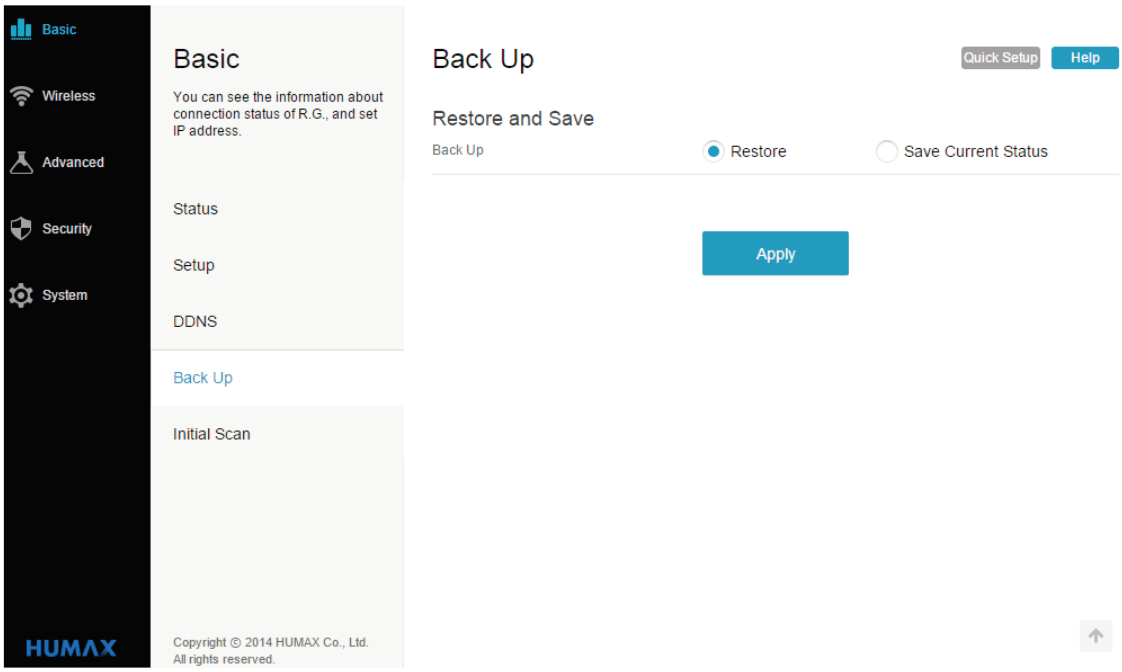
2. Na página DDNS, selecione www.DynDNS.org ou NoIP.com da lista DDNS Service para ativar o serviço, digite as informações da sua conta e clique em Apply.

3. O cliente DDNS irá notificar o serviço DDNS sempre que o endereço IP da WAN mudar, para que seu nome de host escolhido seja resolvido adequadamente pelos hosts.

Backup de configuração

Basic → Back Up

Você pode salvar a configuração atual do gateway residencial em um PC local. Você pode restaurar essas configurações se precisar restaurar uma determinada configuração ou se recuperar de alterações que você possa ter feito.



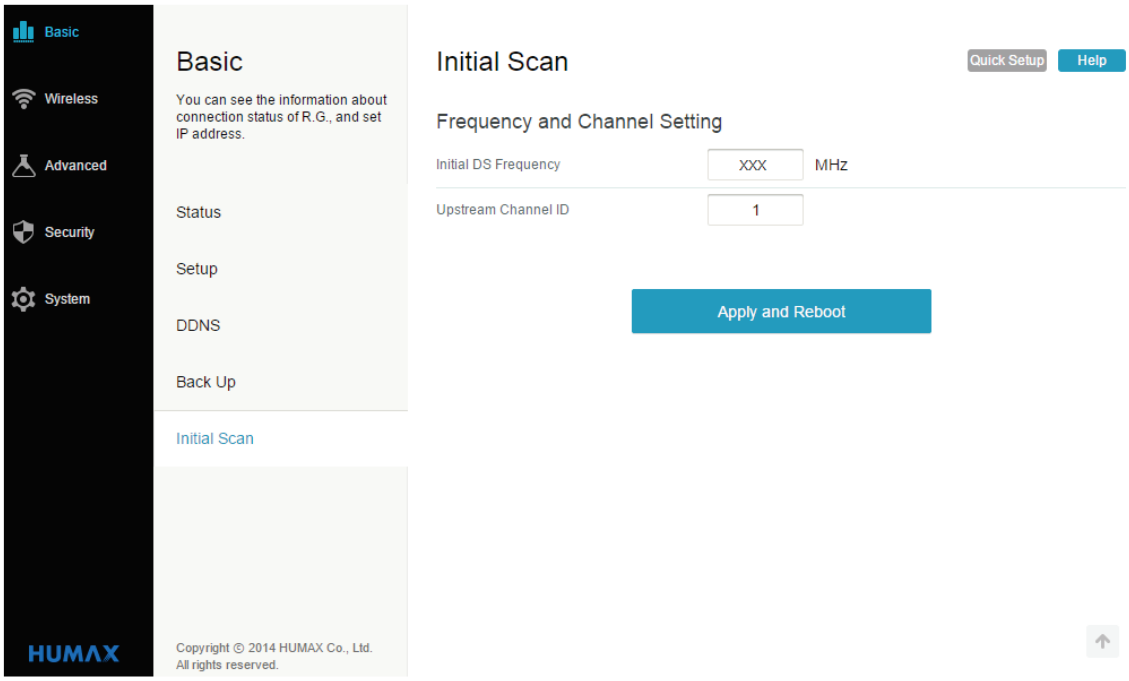
Para restaurar a configuração anterior, selecione a opção Restore e siga o processo para recuperar as configurações anteriores. Para fazer o backup da configuração atual, selecione Save Current Status.

Nota: Uma vez que os ajustes estejam restaurados, o seu produto será reiniciado.

Status de Digitalização Inicial

Basic → Digitalização inicial

Você pode configurar a frequência de inicialização do seu produto.



Configuração de frequência e canal

- Initial DS Frequency: Introduza a frequência à jusante.
- Upstream Channel ID: Digite o ID do canal à montante.

Clique em Apply and Reboot para iniciar a digitalização da rede a cabo, começando com os valores de entrada.

Nota: Essa página é apenas para o fornecedor do serviço. Não altere os valores de entrada se você não estiver familiarizado com esse tipo de operação.

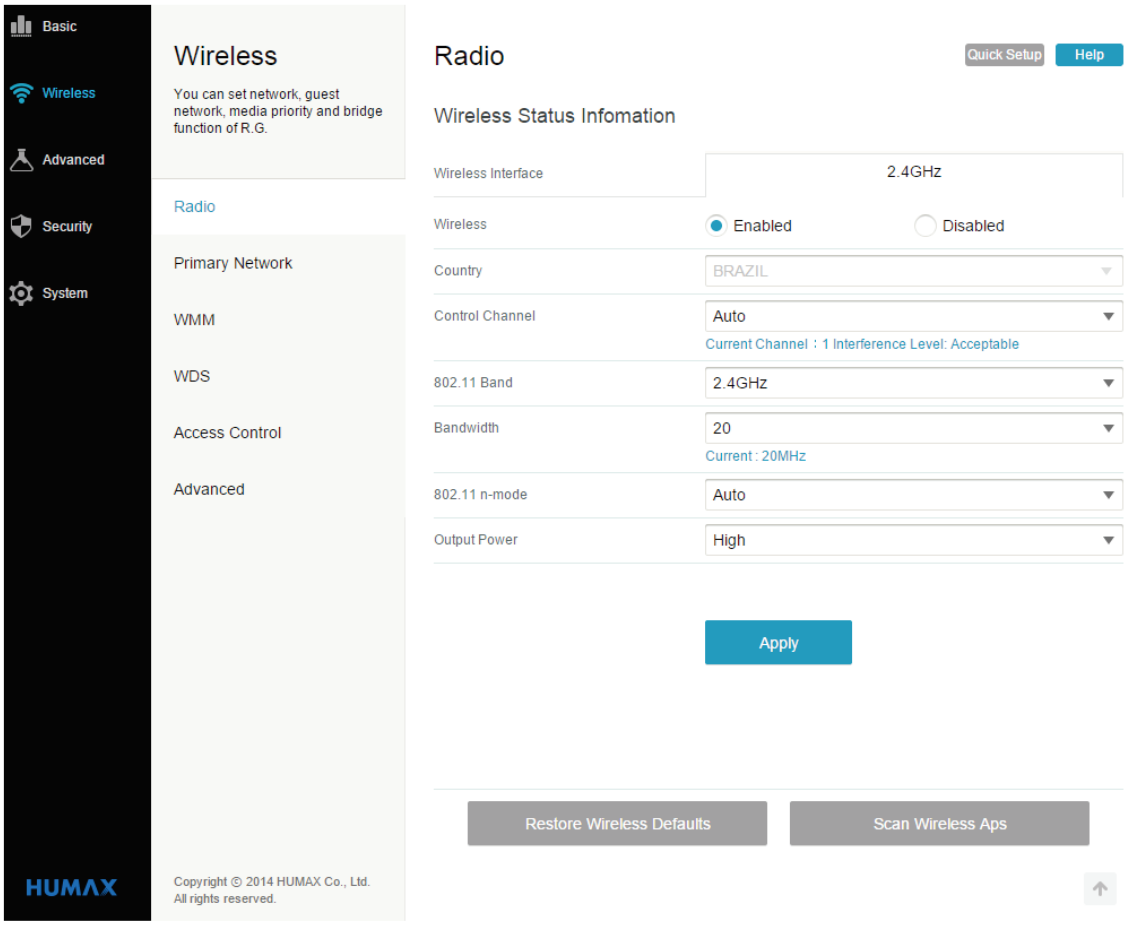
O produto também funciona como um ponto de acesso (AP) sem fio IEEE 802.11.

Quando uma placa de rede sem fio é instalada, o conjunto completo das páginas de configuração da rede sem fio descritas abaixo será exibido no menu Wireless.

Configurações de rádio

Sem fio → Rádio

Você pode configurar os parâmetros físicos de sua rede sem fio.



Informações de Status sem fio

- Wireless: Selecione Enabled para ativar a interface sem fio.
- Country: O seu país é exibido para restringir o conjunto de canais baseados nos requisitos regulamentares do país.
- Control Channel: Selecione o canal de controle para a operação AP. A lista de canais disponíveis depende do país selecionado.
- 802.11 Band: Selecione se o rádio opera em 2,4 GHz ou 5 GHz. Pode haver menos interferência de outras redes sem fio e dispositivos domésticos na faixa de 5 GHz, mas dispositivos 802.11b /g não podem se conectar.
- Bandwidth: Canais 802.11b/g têm apenas amplitude de 20 MHz. Canais 802.11n podem ter amplitude de 40 MHz. Há alguns problemas de compatibilidade retroativa com canais de 40 MHz. Estas questões são mais suscetíveis de serem encontradas na faixa de 2,4 GHz, onde dispositivos legados (802.11b /g) podem estar operando usando canais de 20 MHz.
- 802.11n-mode: Selecione Auto para usar o 802.11n-mode, que permite aumentar a velocidade da rede.
- Output Power: Selecione a potência de saída.

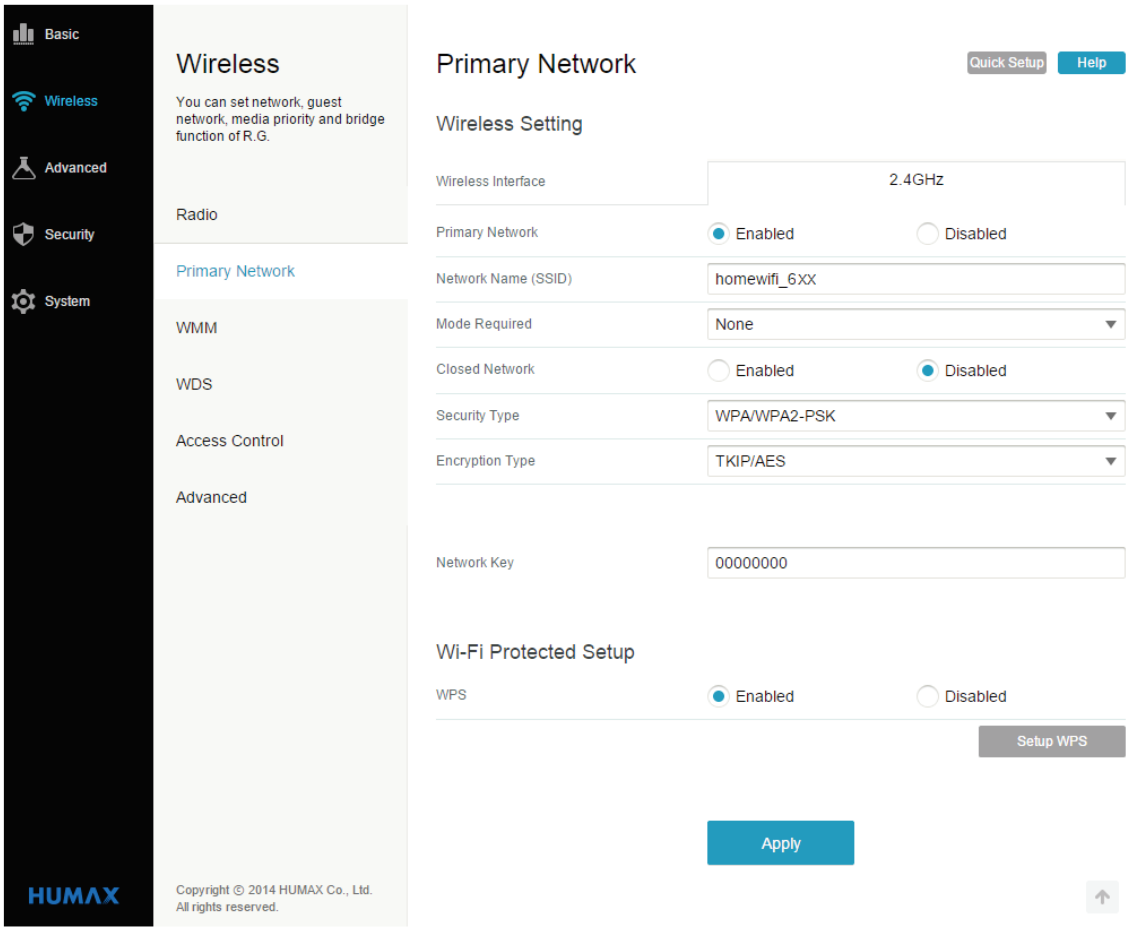
Clique em Restore Wireless Defaults para apagar todas as configurações e redefini-las para os valores padrão.

Clique em Scan Wireless APs para forçar o ponto de acesso a digitalizar outros APs dentro do intervalo de recepção.

Configurações de Rede Primária

Sem fio → Rede Primária

Você pode configurar a rede primária e suas configurações de segurança.



Configuração Sem Fio

- Primary Network: Selecione Enabled ou Disabled para definir o modo de operação da rede primária.
- Network Name (SSID): Digite seu nome de rede para a rede primária. O nome da rede deve ter mais de 8 caracteres e idênticos aos de todos os dispositivos em uma rede sem fio.
- Mode Required: Você pode configurar conexões 802.11g/n/ac do dispositivo sem fio em sua rede sem fio.

  None: Você pode conectar todos os dispositivos independentemente de serem 802.11g/n/ac, mas a velocidade sem fio pode variar dependendo do dispositivo a ser conectado.

  ERP(only 802.11g): permite dispositivos que suportam 802.11g, apenas.

  HT(only 802.11n): permite dispositivos que suportam 802.11n, apenas.

  VHT(only 802.11ac): permite dispositivos que suportam 802.11ac, apenas.
- Closed Network: Selecione Enabled para ocultar o nome da rede. Você pode impedir que outros usuários detectem a rede quando tentam exibir as redes sem fio disponíveis.
- Security Type: Defina o modo pre-shared key.

  WPA-PSK: O modo Pre-Shared Key do algoritmo WPA que não exige o uso de um servidor RADIUS. Este também é conhecido como WPA Personal. WPA e WPA-PSK não podem ser utilizados ao mesmo tempo.

  WPA2-PSK: O modo Pre-Shared Key de WPA2, também conhecido como o WPA2 Personal. WPA e WPA2-PSK não podem ser utilizados ao mesmo tempo. WPA2-PSK e WPA-PSK podem ser usados ao mesmo tempo para proporcionar compatibilidade com dispositivos que não suportam WPA2.

WPA/WPA2-PSK: O modo Pre-Shared Key do algoritmo WPA que não exige o uso de um servidor RADIUS. Este também é conhecido como WPA Personal. WPA e WPA-PSK não podem ser utilizados ao mesmo tempo.

WPA2-Enterprise: Uma forma avançada de WPA que é mais segura. Este é o modo Enterprise de WPA2 que requer o uso de um servidor RADIUS. WPA2 e WPA podem ser usados ao mesmo tempo para proporcionar compatibilidade com dispositivos que não suportam WPA2.

WPA/WPA2-Enterprise: AES prevê criptografia mais forte, enquanto que TKIP fornece criptografia forte com melhor compatibilidade com versões anteriores. O modo TKIP + AES permite que clientes de TKIP e AES se conectem.

O modo Pre-Shared Key de WPA2, também conhecido como o WPA2 Personal.

WPA e WPA2-PSK não podem ser utilizados ao mesmo tempo. WPA2-PSK e WPA-PSK podem ser usados ao mesmo tempo para proporcionar compatibilidade com dispositivos que não suportam WPA2.

- Encryption Type: Defina o modo de criptografia ao usar qualquer um dos esquemas de autenticação WPA.

  AES prevê a criptografia mais forte.

  TKIP/AES fornece criptografia forte com melhor compatibilidade com versões anteriores.

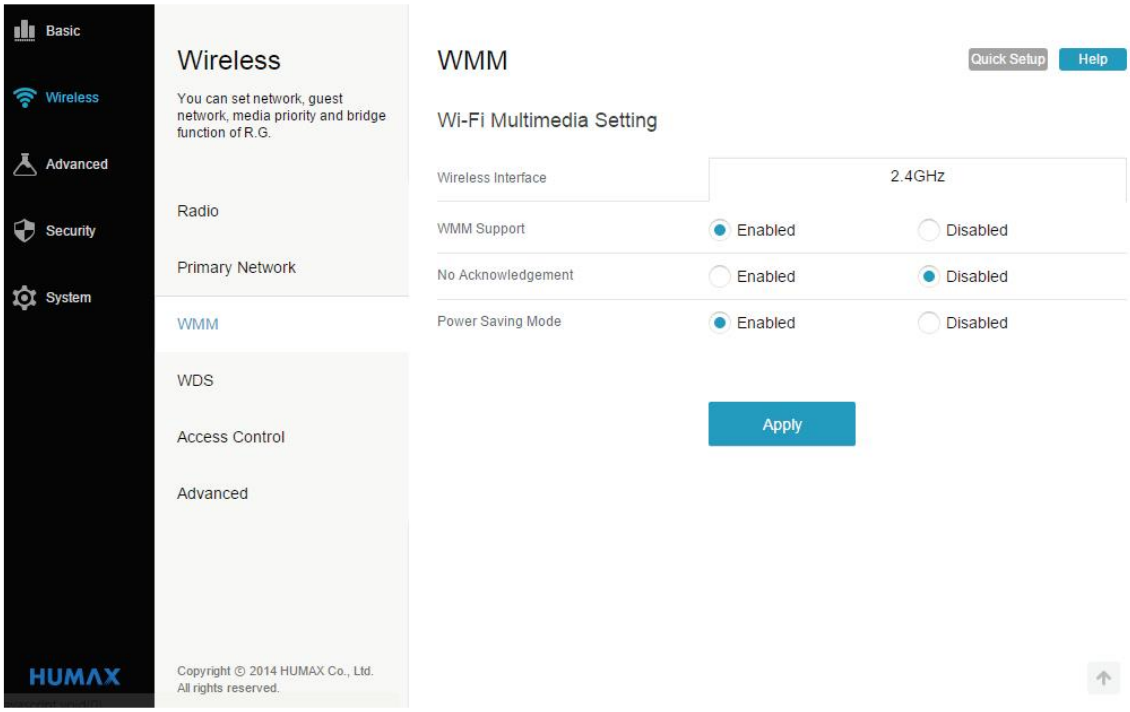
Configuração protegida de Wi-Fi

- WPS: Selecione Enabled para configurar uma rede sem fio segura e adicionar dispositivos sem fio em sua rede sem fio. Pressione o botão Setup WPS para configuração da conexão sem fio WPS.

Configurações WMM

Sem fio → WMM

Você pode configurar o Wi-Fi Multimedia (WMM). WMM é uma implementação de Qualidade de Serviço (QoS) que é definida pelo padrão IEE 802.11e .



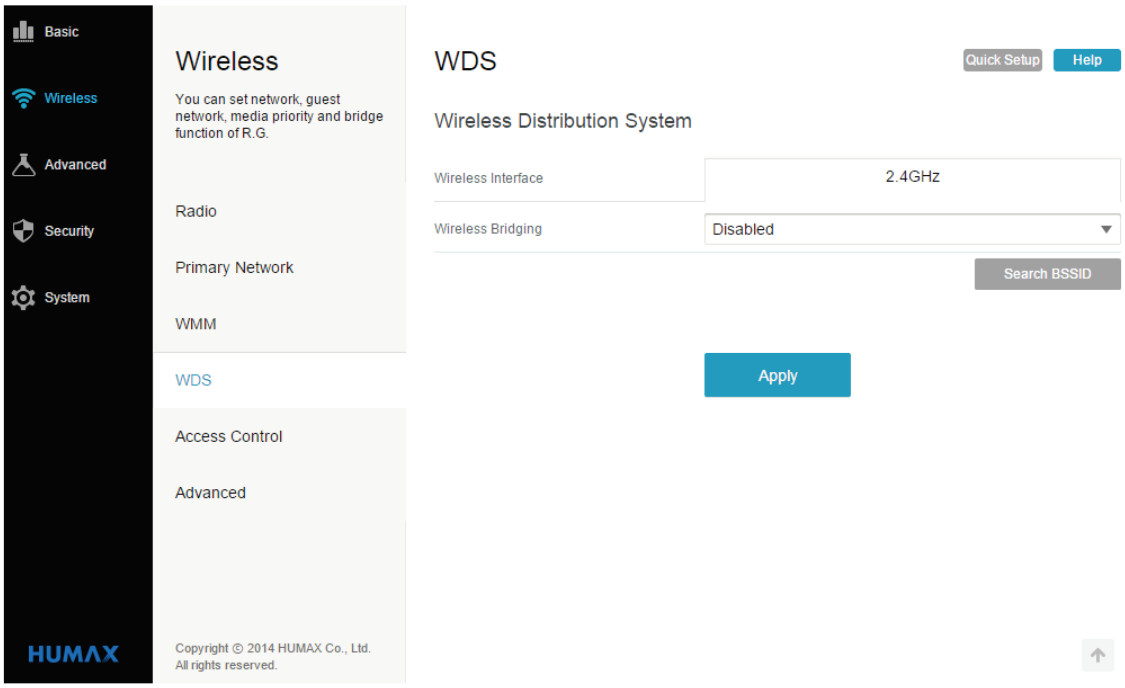
Configuração de Wi-Fi Multimedia

- WMM Support: Selecione Enabled para transmitir ou receber multimídia através da rede sem fio.
- No Acknowledgement: Selecione Enabled para não receber WMM ACK.
- Power Saving Mode: Selecione Enabled para entrar em modo de espera automaticamente, se o produto não funcionar por um tempo predefinido.

Configurações WDS

Sem fio → WDS

Você pode configurar o Wireless Distribution System (WDS), que também é conhecido como ponte sem fio. WDS permite que você conecte múltiplos pontos de acesso sem fio em conjunto com uma única rede usando conexões ponto-a-ponto sem fio.



Sistema de Distribuição Sem Fio

- Wireless Bridging: Defina a ponte sem fio para WDSMaster ou WDSSlave.

  No modo WDS master, o modem roteador é o mestre de um grupo de estações sem fio em modo bridge. Em seguida, todo o tráfego é definido para este mestre, em vez de outros pontos de acesso.

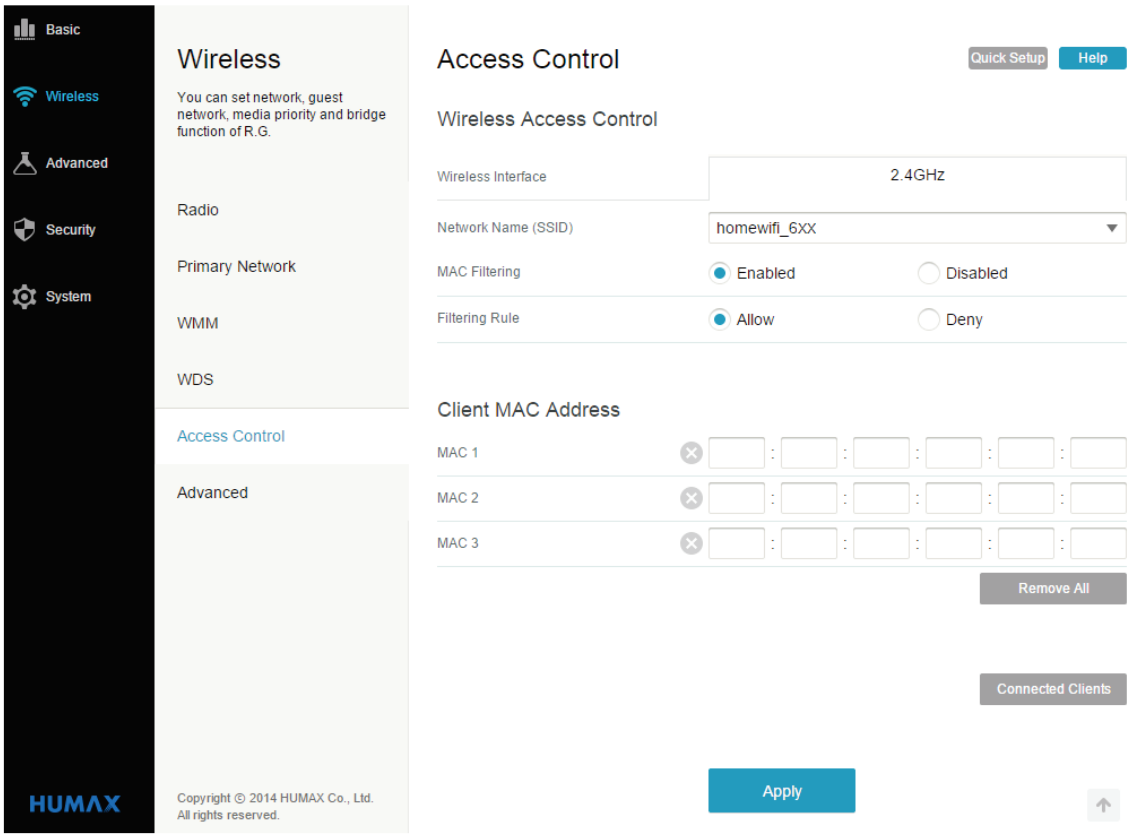
  No modo WDS slave, o modem roteador se comunica com outra estação sem fio em modo bridge.

- Remote Bridges: Digite os endereços MAC da ponte remota autorizados a estabelecer uma ponte sem fios. Até 4 pontos podem ser conectadas. Em geral, você também terá de introduzir o seu endereço MAC de AP na ponte remota.

Configurações de acessibilidade

Sem fio → Access Control

Você pode controlar quais clientes sem fio podem acessar sua rede sem fio. Ele também fornece informações sobre os clientes sem fio conectados ao seu ponto de acesso.



Controle de Acesso Sem fio

- Network Name (SSID): Selecione sua rede para definir o acesso sem fios a ela.
- MAC Filtering: Selecione Enabled ou Disabled para definir se o cliente sem fio com o endereço MAC é permitido ou negado ao acesso sem fio. Para permitir todos os clientes, selecione Disabled.
- Filtering Rule: Selecione Allow ou Deny para definir a acessibilidade para o dispositivo do cliente.

Endereço MAC do cliente

Esta configuração é indicada se você selecionar Enabled para a filtragem de MAC no Controle de Acesso Sem Fio.

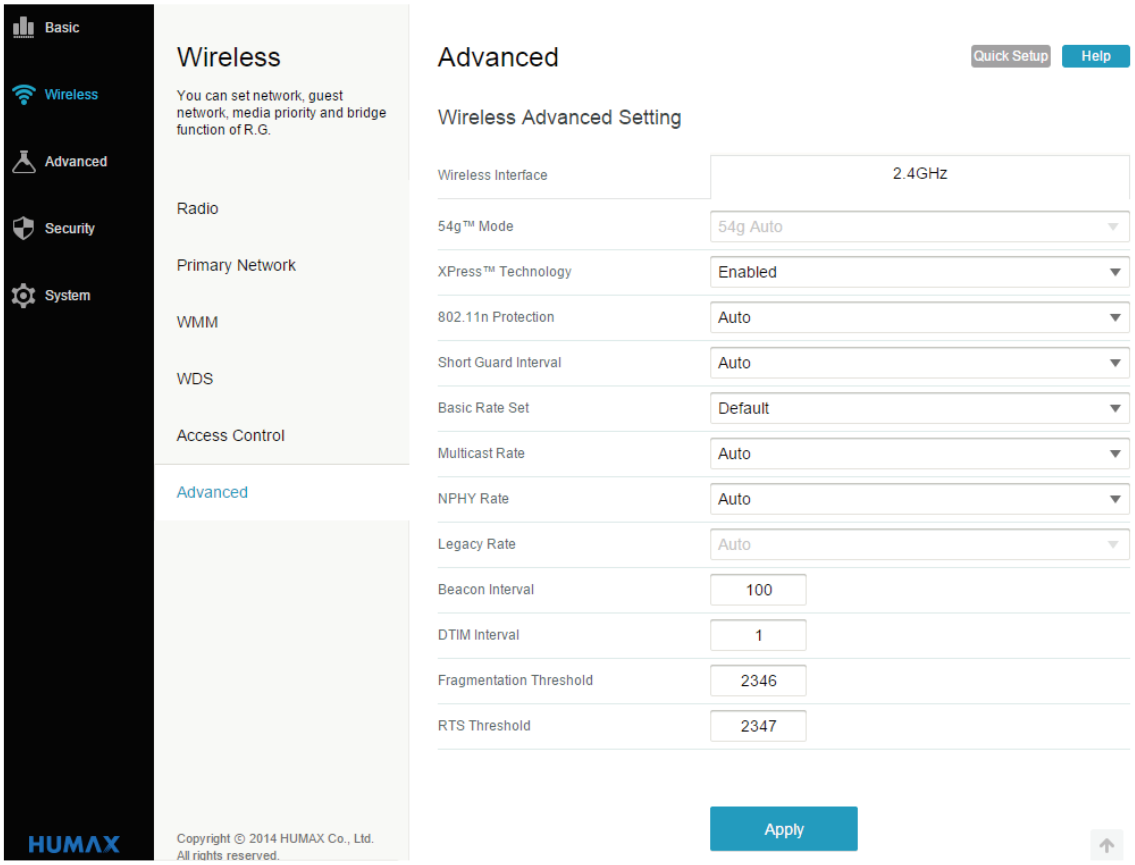
- MAC 1/2/3: Digite os endereços MAC do cliente sem fio para permitir ou negar acesso baseado na regra de filtragem

Para ver os clientes sem fio conectados, clique em Connected Clients. Você pode verificar as informações do cliente, como ID do cliente, endereço MAC, a intensidade do sinal e assim por diante.

Configurações avançadas sem fio

Sem fio → Advanced

Você pode definir outras configurações de rede sem fio. A maioria dos usuários não tem necessidade de alterar essas configurações.



Configuração avançada sem fio

- 54g™ Mode: Modo de rede é configurado para 54g Auto.

  54g Auto aceita clientes em 54g, 802.11g e 802.11b, mas otimiza o desempenho com base no tipo de clientes conectados.

- XPress™ Technology: Você pode ativar o método exclusivo HUMAX de reconhecimento da estrutura de bloco para quadros 802.11g. Este recurso pode melhorar a produtividade, mas pode causar problemas.
- 802.11n Protection: Esta opção é semelhante à proteção de 54g, exceto que se aplica aos dispositivos do padrão 802.11n.
- Short Guard Interval: Você pode definir o intervalo de guarda para evitar a perda de dados resultante de interferência ou atrasos em vários trajetos.
- Basic Rate Set: Você pode verificar quais taxas são anunciadas como taxas básicas e definir todas as taxas disponíveis como taxas básicas. Por padrão usa-se os padrões do driver.
- Multicast Rate: Você pode definir a taxa de multicast em que pacotes multicast são transmitidos para as estações. Pacotes Multicast não são reconhecidos.
- NPHY Rate: Você pode selecionar a taxa de 802.11n a ser aplicada em todos os pacotes unicast.
- Legacy Rate: Você pode forçar a taxa na qual a AP funciona. Esta opção é ativada quando o modo 802.11n é definido como Off.
- Beacon Interval: Você pode definir o intervalo de beacon em milissegundos para AP. O padrão é 100, o que é bom para quase todas as aplicações.

- DTIM Interval: Você pode definir o intervalo de despertar para clientes em modo de economia de energia. Quando um cliente é executado no modo de economia de energia, os valores mais baixos oferecem maior desempenho, mas resultam em menor vida útil da bateria do cliente, enquanto que valores mais altos proporcionam desempenho inferior, mas resultam em uma maior vida útil da bateria.
- Fragmentation Threshold: Você pode definir o limite de fragmentação. Os pacotes que excedam este limite são fragmentados em pacotes não maiores que o limite antes da transmissão do pacote.
- RTS Threshold: Você pode definir o limite RTS. Os pacotes que excedam este limite fazem com que AP execute uma troca RTS/CTS para reservar o meio sem fio antes da transmissão do pacote.

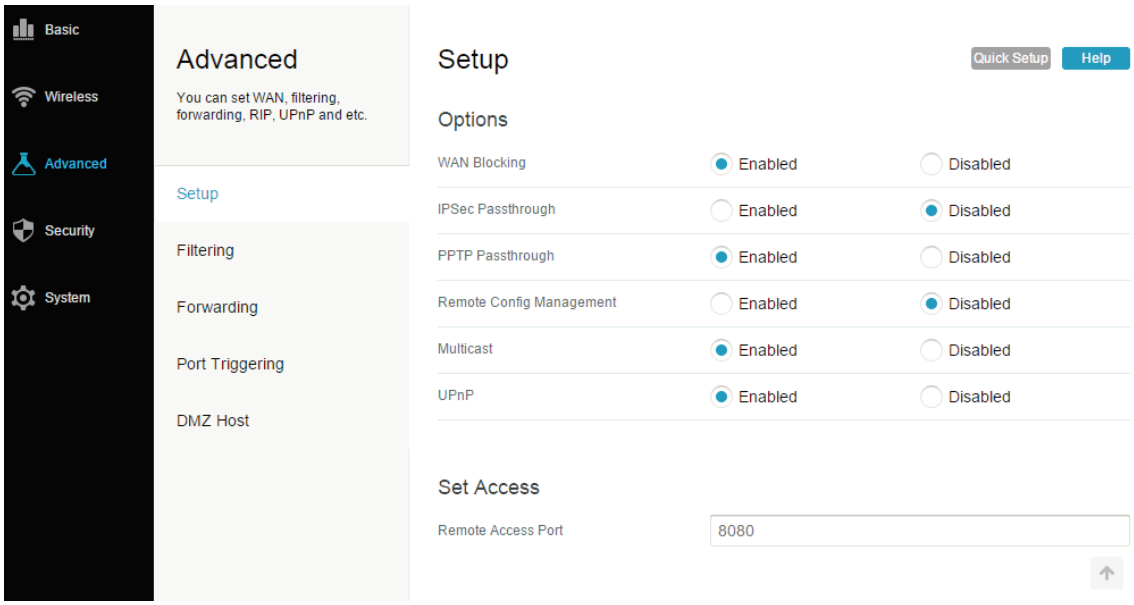
O produto suporta funcionalidades avançadas adicionais, por exemplo:

- Suporte a modos de ativação opcionais de WAN blocking, IpSec pass-through, PPTP pass-through, remote management, multicast e UPnP
- Filtragem de endereços IP LAN, endereço MAC e número de porta
- Encaminhamento e acionamento a partir de WAN para LAN
- Suporte a DMZ hosting (ou host exposto)

Configurações avançadas

Advanced → Setup

Você pode operar o seu produto em vários modos que ajustam a forma como o dispositivo direciona o tráfego IP.

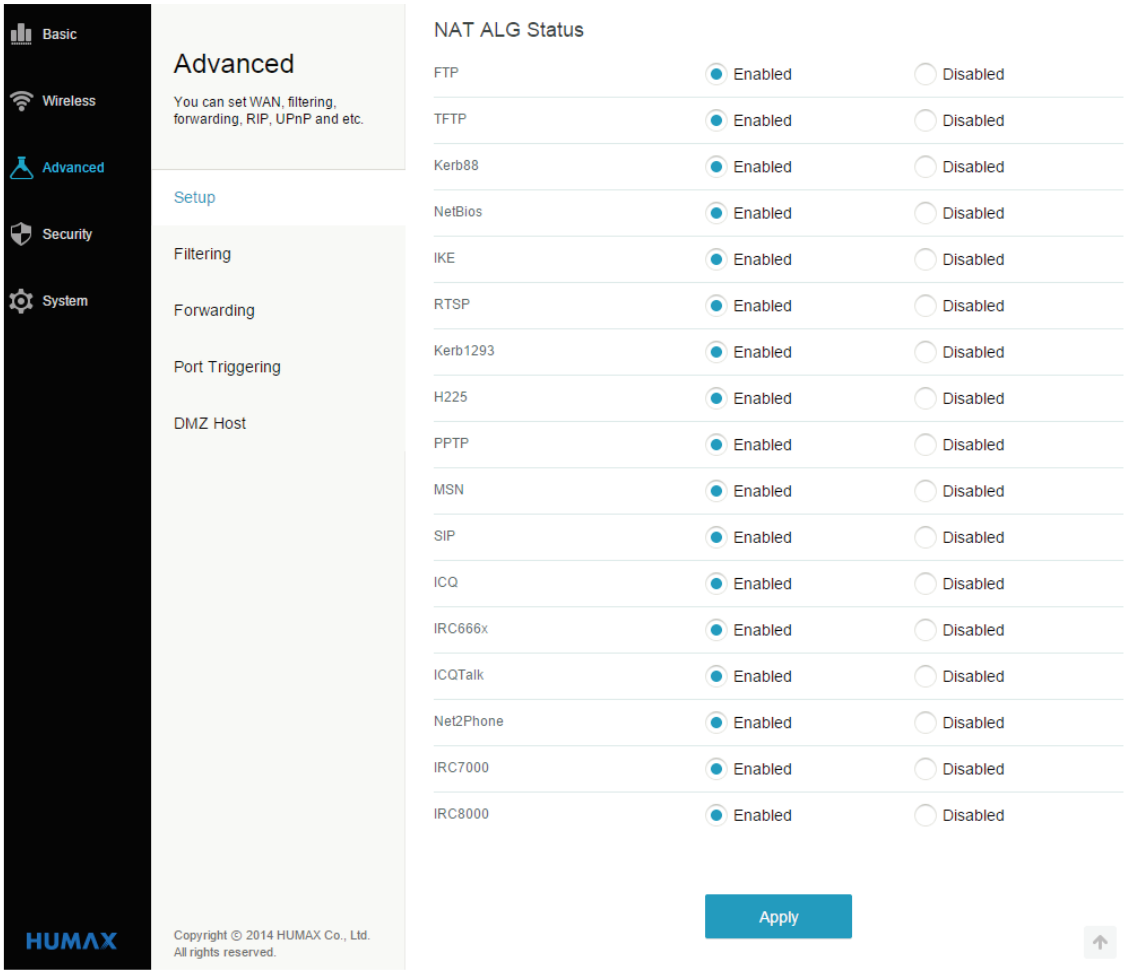


Opções

- WAN Blocking impede que o gateway residencial ou os PCs por trás dele estejam visíveis para WAN. Por exemplo, pings para o endereço IP WAN do gateway residencial ou dos PCs por trás dele não são devolvidos. Portanto, será mais difícil para hackers descobrirem seu endereço IP WAN para iniciar um ataque em sua LAN privada.
- IPSec Passthrough e PPTP Passthrough habilitam esses protocolos para serem usados através do gateway residencial, de tal modo que um dispositivo VPN ou software pode se comunicar adequadamente com a WAN.
- Remote Config Management permite que o gateway residencial seja administrado (configurado) a partir da WAN via surfing para o endereço IP WAN na porta 8080 do gateway residencial de qualquer lugar na Internet (por exemplo, na janela de URL do navegador insira http://WanIPAddress:8080/ para acessar o gateway residencial remotamente).
- Multicast permite que tráfego específico de Multicast (identificado por um endereço específico de multicast) seja transmitido para e a partir do computador da rede privada por trás do gateway residencial.
- UPnP permite o agente UPnP no gateway residencial. Se você estiver executando uma aplicação CPE que requer UPnP, selecione Enabled.

Definir acesso

- Remote Access Port: Digite o número da porta para o acesso remoto. Para reforçar a segurança, digite uma porta (1~65535) que não a 80.



NAT ALG Status

NAT ALG significa tradução de endereços de rede e gateway de nível de aplicação. Você pode definir estes componentes de firewall para ser ativados ou não.

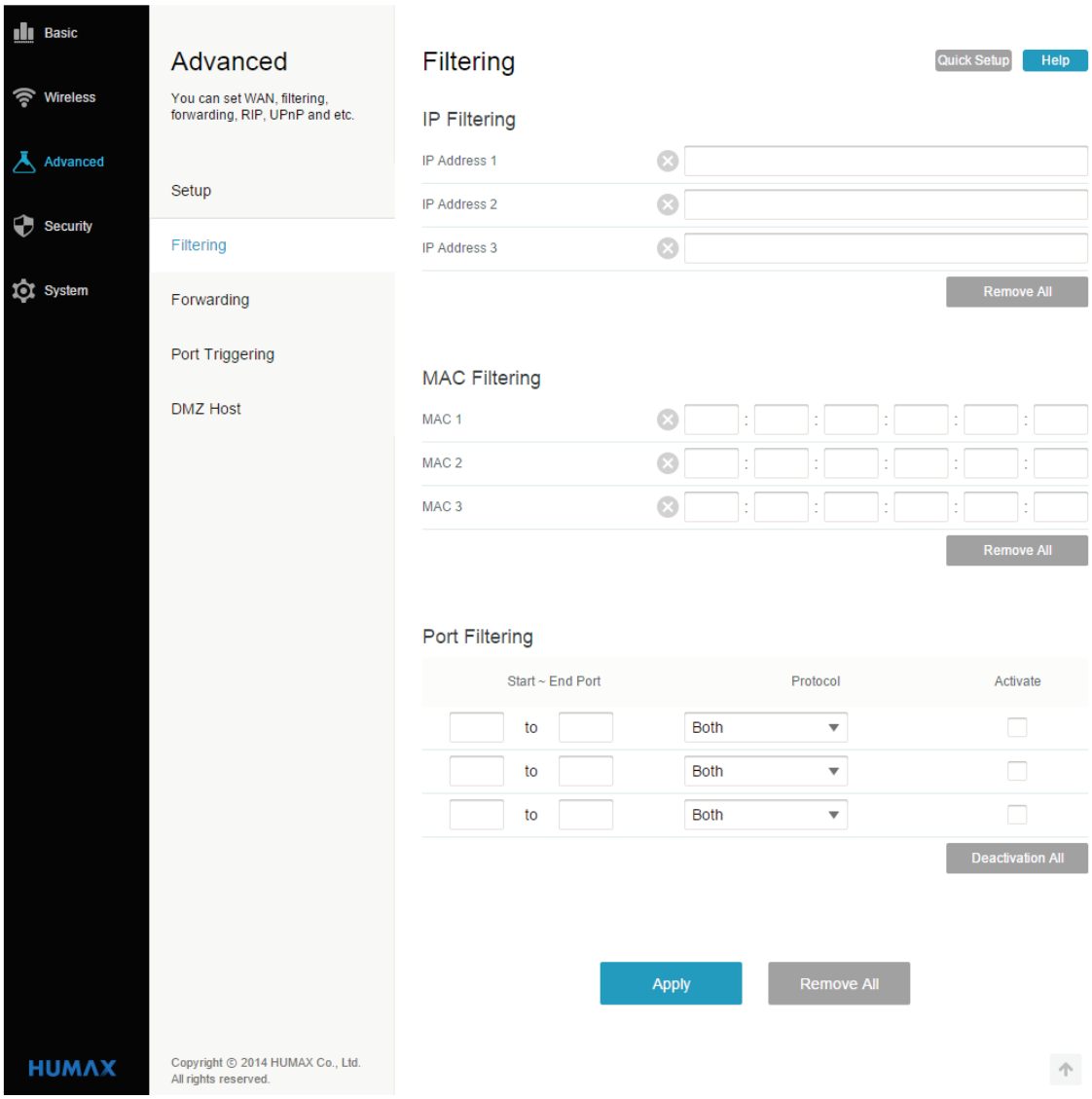
Para ativar uma funcionalidade, clique na opção e, em seguida, Apply. Estas características são alteradas sem a necessidade de reiniciar o sistema.

Nota: As configurações avançadas só são recomendadas para usuários avançados. Se você não estiver familiarizado com o funcionamento, não altere as configurações nesta página.

Filtro

Advanced → Filtering

Você pode configurar o firewall para implementar filtragem de pacotes e assim permitir ou negar tráfego de dados para segurança de dados.



Filtragem por IP

Você pode configurar seu gateway residencial para evitar que computadores locais obtenham acesso à WAN, especificando os endereços IP que devem ser filtrados.

Digite os endereços de IP para configurar quais PCs locais têm o acesso negado para WAN.

Filtragem por MAC

Você pode impedir que os computadores enviem tráfego TCP/UDP de saída para WAN através de seu endereço MAC.

Isso é útil para o fato de que o endereço MAC de uma placa de rede específica nunca muda, ao contrário de seu endereço de IP que pode ser atribuído pelo servidor DHCP ou codificado para vários endereços ao longo do tempo.

Filtragem de portas

Você pode impedir que os computadores enviem tráfego TCP/UDP de saída para WAN através dos números específicos da porta IP.

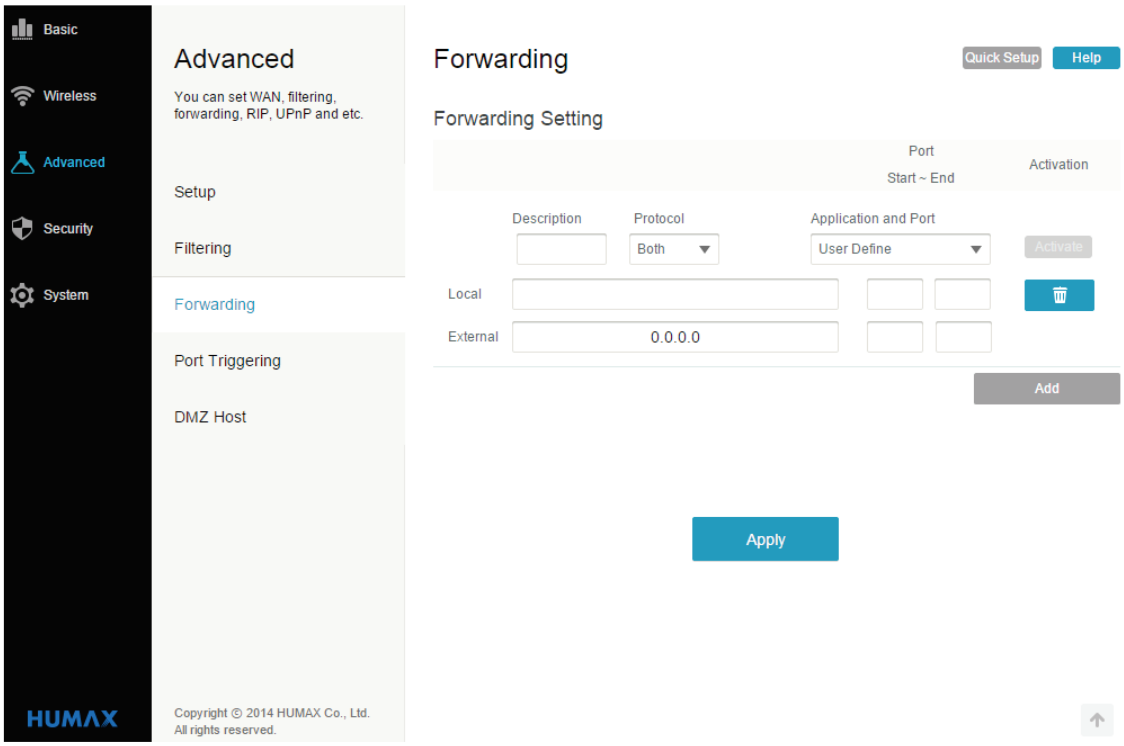
Introduza um intervalo inicial e final de portas para determinar qual o tráfego TCP/UDP é permitido para a WAN em uma base por porta.

Nota: Os intervalos especificados de portas são bloqueados para todos os PCs e esta definição não é o endereço IP ou o endereço MAC específico.

Encaminhamento de porta

Advanced → Forwarding

Você pode executar um servidor de acesso público na LAN, especificando o mapeamento de portas TCP/UDP para um computador local.



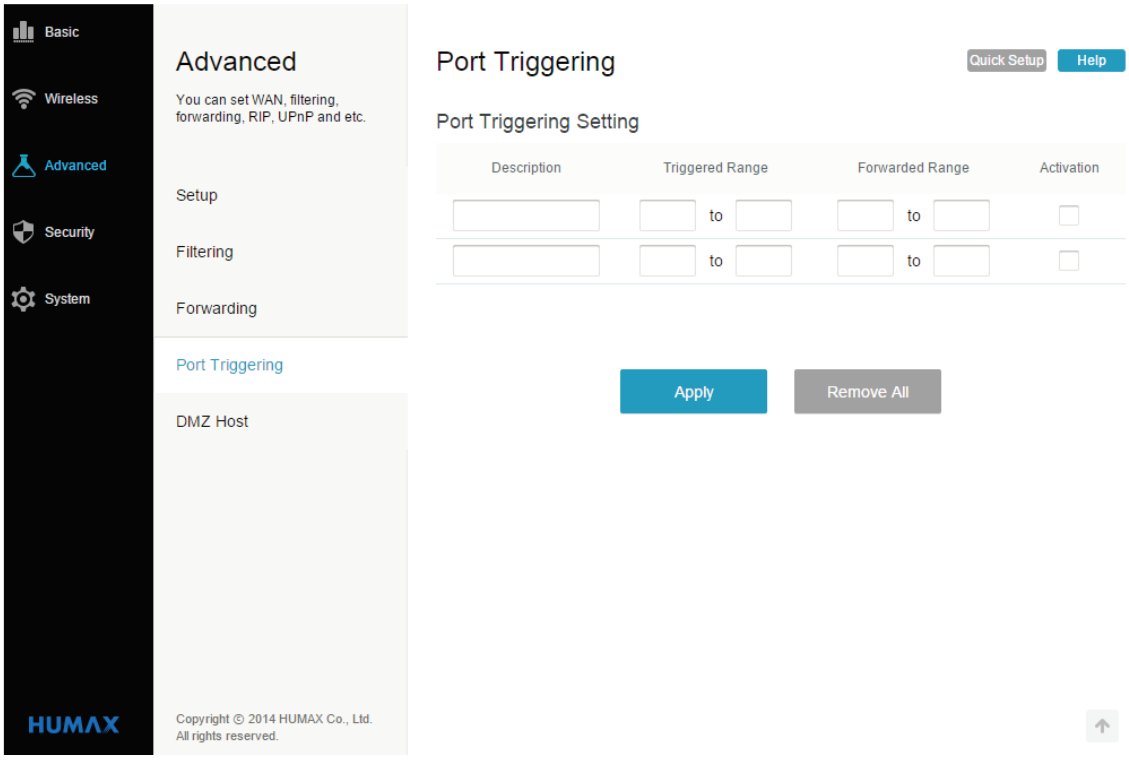
Para especificar um mapeamento, introduza o intervalo de números de porta que deve ser transmitido localmente, e o endereço IP de onde o tráfego para as portas deve ser enviado.

Nota: Se você quiser apenas uma única especificação de porta, insira o mesmo número de porta nas portas de início e de final para aquele endereço IP.

Acionamento de porta

Advanced → Port Triggering

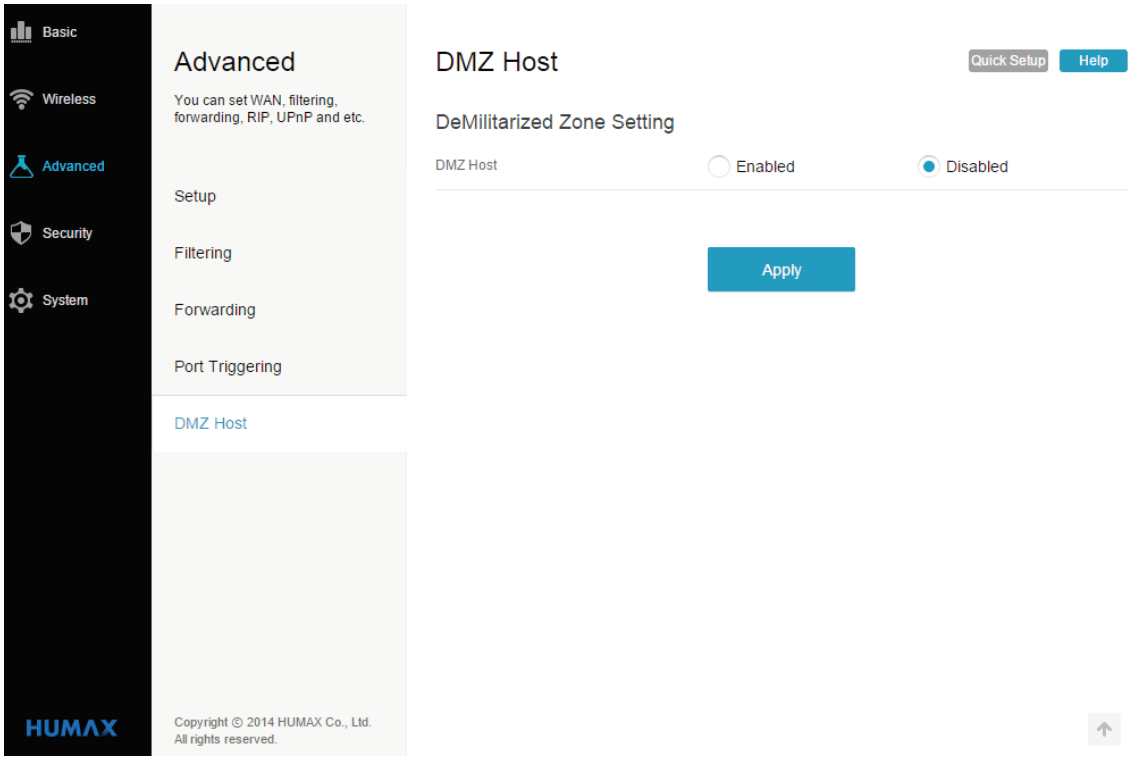
Port Triggering é similar ao port forwarding exceto que não são portas estáticas mantidas abertas o tempo todo. Quando o gateway residencial detecta dados de saída em um número de porta IP definido no intervalo acionado, as portas resultantes definidas no intervalo encaminhado são abertas para receber dados (ou às vezes chamadas de portas bidirecionais). Se nenhum tráfego de saída for detectado no intervalo acionado das portas por 10 minutos, as portas irão se fechar. Este é um método mais seguro para abrir portas específicas para aplicações especiais (por exemplo, programas de videoconferência, jogos interativos, transferência de arquivos em programas de bate-papo, etc.), porque são disparadas dinamicamente e não mantidas abertas constantemente ou erroneamente deixadas abertas por causa do administrador do roteador e expostas a potenciais hackers.



DMZ Hosting

Advanced → DMZ Hosting

DMZ (zona desmilitarizada) Host (também comumente chamado de "host exposto") permite que você especifique o destinatário padrão de tráfego WAN que o NAT não consegue converter para um computador local conhecido. Também pode ser descrito como um computador ou pequena sub-rede que fica entre a LAN privada confiável e a Internet pública não confiável.



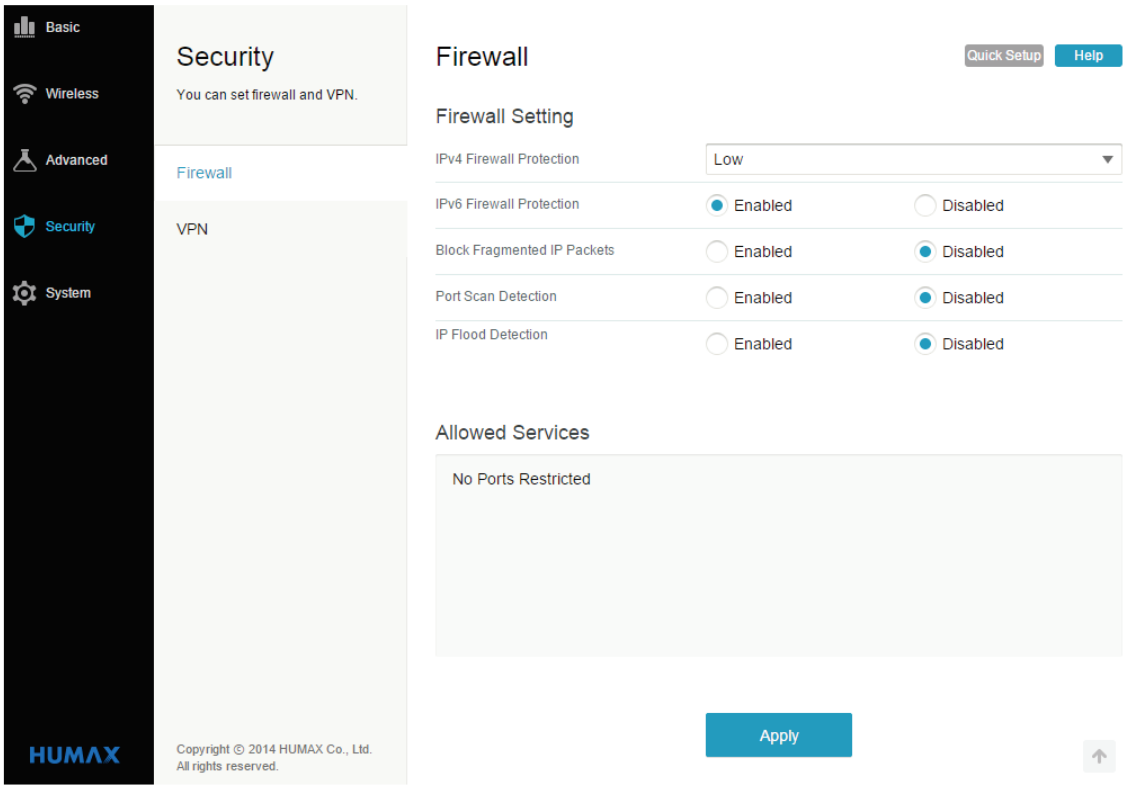
Você pode configurar um PC para ser o DMZ host. Essa configuração é geralmente utilizada para aplicações para PCs usando aplicações de problema que usam números de porta aleatórios e não funcionam corretamente com acionamentos de porta específicos ou configurações de encaminhamento de portas mencionados anteriormente. Se um computador específico é definido como um DMZ host, lembre-se de definir esta opção para 0 quando terminar com a aplicação necessária, uma vez que este PC será efetivamente exposto à Internet pública, embora ainda esteja protegido contra ataques de Denial of Service (DoS) através do firewall.

O gateway residencial contém um aplicativo de firewall embutido para proteger a LAN privada de ataques maliciosos a partir da interface WAN.

Configurações de Firewall

Security → Firewall

A página da web Filter tem várias configurações relacionadas ao bloqueio ou exclusivamente permitindo que diferentes tipos de dados passem através do gateway residencial da WAN para a LAN.



Configuração de Firewall

- IPv4 Firewall Protection: Selecione a opção de proteção de firewall.

  Low não bloqueia quaisquer serviços/portas, no entanto, protege contra pacotes inválidos e ataques conhecidos.

  Medium pode fazer com que o firewall interrompa um pacote, a menos que esteja em uma porta específica de serviços autorizados. Os serviços permitidos estão listados na mesma página.

  High é semelhante ao Medium , mas permite o acesso a um número ainda menor de serviços.

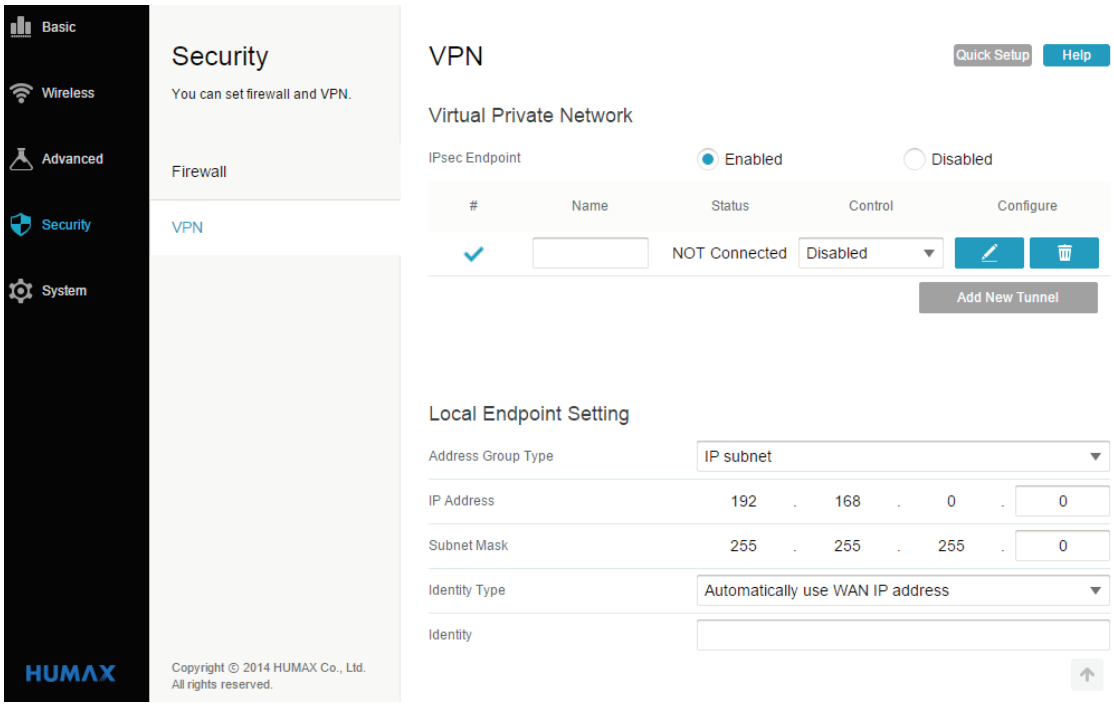
  Disabled permite que todo o tráfego passe.

- IPv6 Firewall Protection: Selecione Enabled para definir a proteção de firewall IPv6.
- Block Fragmented IP Packets: Selecione Enabled para evitar que todos os pacotes IP fragmentados passem pelo firewall.
- Port Scan Detection: Selecione Enabled para detectar e bloquear atividades de digitalização de porta tanto na LAN quanto na WAN.
- IP Flood Detection: Selecione Enabled para fazer o firewall detectar ataques de IP flood.

Configuração de VPN

Security → VPN

Você pode configurar vários túneis VPN em vários PCs clientes. Diferentes túneis podem ser configurados e armazenados, mas não habilitados para facilidade de uso com conexões e/ou PCs clientes que não são usados constantemente. Para cada configuração do túnel, os seus parâmetros exclusivos de IPsec são armazenados usando o menu IPsec Settings na parte inferior da página.



Rede Privada Virtual

- IPsec Endpoint: Selecione Enabled ou Disabled para o IPsec endpoint mode.
- Nome: Exibe o nome do túnel definido pelo usuário
- Status: Exibe o estado de conexão atual
- Control: Selecione uma opção com base no estado atual da conexão do túnel

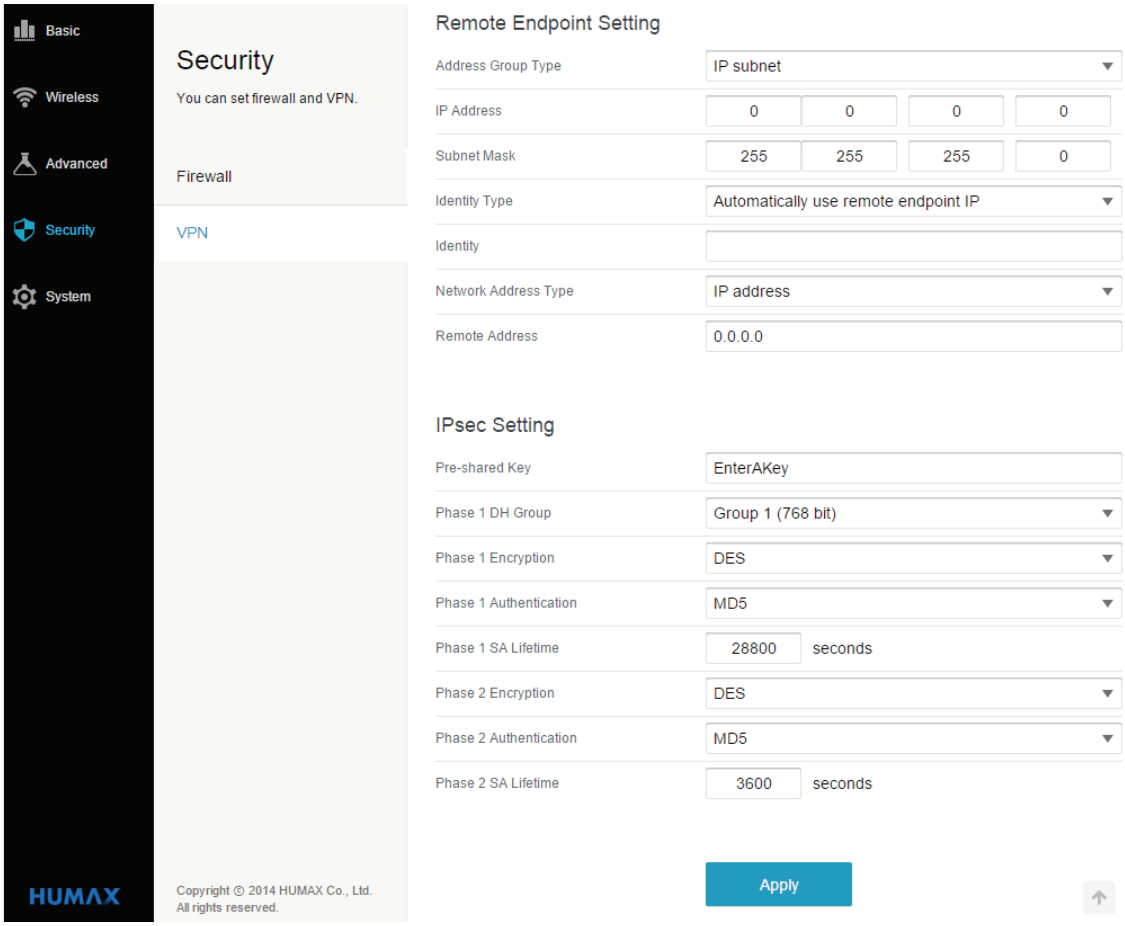
  Selecione Enabled para ativar o servidor VPN.

  Selecione Disabled para desativar o servidor VPN.

  Selecione Connect para se conectar com o servidor VPN.

  Selecione Disconnect para se desconectar do servidor VPN.
- Configure: Clique em Edit ou Delete para configurar o túnel VPN.

Clique no botão Add New Tunnel para criar uma nova configuração de túnel.



Configuração do Ponto Final Local

- Address Group Type: O grupo de acesso VPN local pode ser definido aqui para ser um único endereço IP específico de um computador, um intervalo de endereços IP para cobrir uma pequena gama de computadores, ou toda sub-rede/rede.

  Selecione IP Subnet para inserir a sub-rede e as informações de máscara.

  Selecione Single IP para inserir apenas o endereço IP específico.

  Selecione IP address range para introduzir os endereços IP de início e fim para compensar pelos endereços de IPs consecutivos que terão acesso ao túnel.

- IP Address: Digite o ponto final do endereço IP em sua LAN para definir a VPN.
- Subnet Mask: Insira a máscara de sub-rede.
- Identity Type: Você pode definir o tipo de identidade local para usar automaticamente o endereço IP WAN do roteador ou como um usuário de endereço IP especificado, nome de domínio totalmente qualificado (FQDN), ou E-mail.
- Identity: Uma vez que o tipo de identidade é selecionada da lista, a sequência de identidade deve ser inserida aqui. Para o modo IP address, x.x.x.x é inserido. Para FQDN, "yourdomain.com" seria inserido e para email address identity, yourname@yourdomain.com" seria inserido. O Ponto final remoto de VPN no outro lado do túnel deve coincidir com as configurações feitas aqui para seu ponto final remoto.

Configuração do Ponto Final Remoto

Você pode definir o ponto final remoto da mesma forma que na Configuração do Ponto Final Local e, assim, conectar-se à rede remota como se estivesse conectado diretamente à LAN.

- Network Address Type: Selecione IP address ou Fully Qualified Domain Name (FQDN) para o tipo de endereço WAN do ponto final remoto.
- Remote Address: Insira o endereço IP do ponto final remoto ou seu FQDN, dependendo de qual tipo de Endereço de Rede foi selecionado.

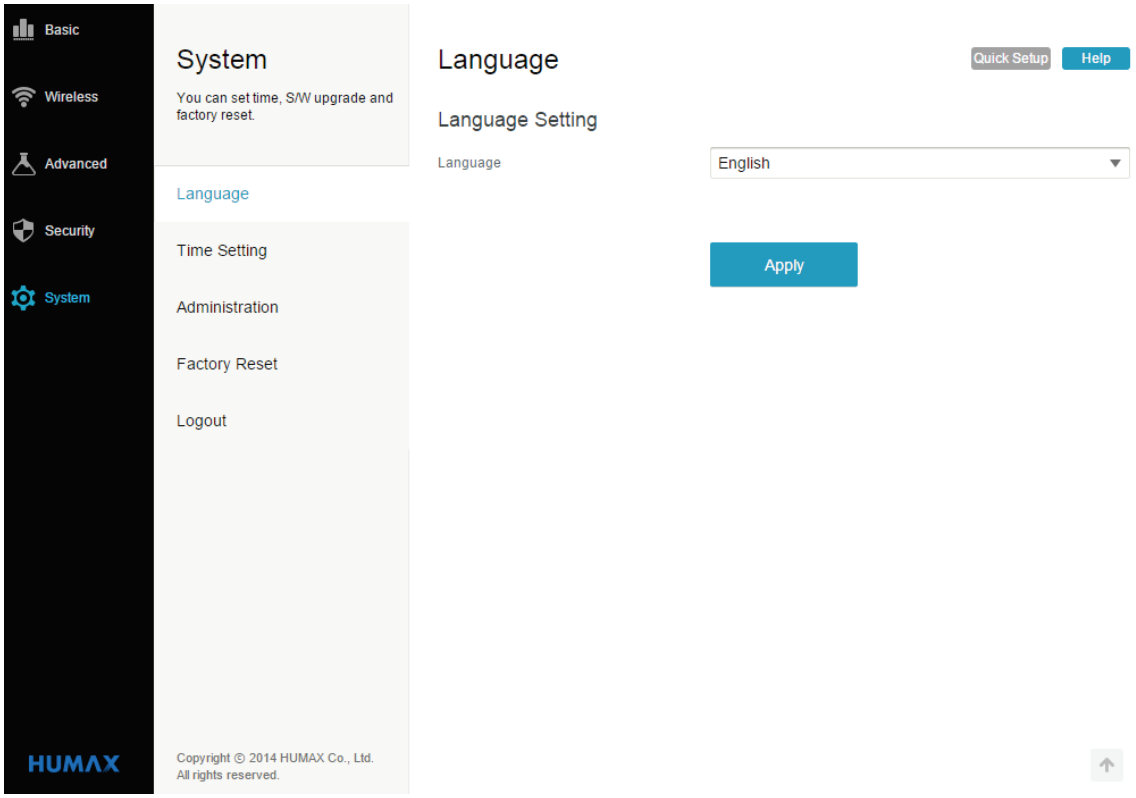
Configuração IPsec

Com túneis VPN, existem duas fases de Associação de Segurança (SA). Fase 1 é usada para criar IKE SA. Após a fase 1 estar completa, Fase 2 é utilizada para criar um ou mais IPsec SAs, que são então utilizados para as sessões principais de IPsec.

- Pre-shared Key: Se um lado do túnel VPN estiver usando um identificador único de firewall (ou Pre-shared Key), esta deve ser inserida no campo "Pre-shared Key".
- Phase 1 DH Group: Selecione um grupo Diffie-Hellman. Diffie-Hellman é uma técnica de criptografia que usa chaves públicas e privadas para criptografia e descriptografia. Quanto maior for o número de bits selecionados, mais segura é a rede.
- Phase 1 Encryption: A criptografia é usada para proteger a conexão VPN entre os terminais. Cinco tipos diferentes de criptografia estão disponíveis. Qualquer forma de criptografia pode ser selecionada, contanto que os pontos finais sejam compatíveis. Uma das definições mais comuns aqui é 3DES; no entanto, AES também é um método de criptografia muito forte.
- Phase 1 Authentication: Autenticação age como outro nível de segurança. SHA é recomendado porque é mais seguro. Ambos os tipos de autenticação podem ser usados, contanto que a outra extremidade do túnel VPN utilize o mesmo método.
- Phase 1 SA Lifetime: Neste campo, a vida útil das chaves rotativas individuais é especificada. Digite o tempo para a chave até que uma nova negociação de chave entre cada ponto final seja negociada. Vidas úteis mais curtas são geralmente mais seguras, uma vez que daria ao atacante uma quantidade menor de tempo para tentar quebrar a chave, mas a negociação da chave não ocupa largura de banda, assim o volume de dados da rede será sacrificado com pequenas vidas úteis. Entradas aqui estão tipicamente na casa dos milhares ou dezenas de milhares de segundos.
- Phase 2 Encryption: A criptografia é usada para proteger a conexão VPN entre os terminais. Cinco tipos diferentes de criptografia estão disponíveis: Qualquer forma de criptografia pode ser selecionada, contanto que os pontos finais sejam compatíveis. Uma das definições mais comuns aqui é 3DES; no entanto, a AES também é um método de criptografia muito forte e recomendado uma vez que é muito difícil de decifrar.
- Phase 2 Authentication: Autenticação age como outro nível de segurança. Os três tipos de autenticação estão disponíveis. SHA é recomendado porque é mais seguro. Ambos os tipos de autenticação podem ser usados, contanto que a outra extremidade do túnel VPN utilize o mesmo método.
- Phase 2 SA Lifetime: Neste campo, a vida útil das chaves rotativas individuais é especificada. Digite o tempo para a chave até que uma nova negociação de chave entre cada ponto final seja negociada. Vidas úteis mais curtas são geralmente mais seguras, uma vez que daria ao atacante uma quantidade menor de tempo para tentar quebrar a chave, mas a negociação da chave não ocupa largura de banda, assim o volume de dados da rede será sacrificado com pequenas vidas úteis. Entradas aqui estão tipicamente na casa dos milhares de segundos.

Configurações do Sistema

Você pode verificar a hora atual do sistema, alterar a senha ou restaurar o produto para as configurações de fábrica.



Idioma

Você pode definir o idioma do sistema.

Configuração da Zona de Fuso horário

Você pode ver a hora atual definido no produto. Vários dispositivos são sincronizados com o mesmo horário.

Administração

Você pode alterar sua senha. Digite uma nova senha e novamente a nova senha. Clique em Apply para salvar suas alterações.

Configuração de Reinicialização de Fábrica

Você pode restaurar o produto para as configurações padrões de fábrica. Para restaurar para os padrões de fábrica, selecione Yes e clique em Apply.

Aviso: Depois de restaurar para os padrões de fábrica, todos os dados do usuário configurados serão apagados.

Logout

Você será automaticamente desconectado.

Especificações

Tamanho (L x P x A)	225 x 155 x 44 (mm)
Peso	440g
Tensão de entrada	12V ⎓ 1.5A
Consumo de energia	17W
Temperatura operacional	0° a 40 °C

Nota: As especificações estão sujeitas a alterações sem aviso prévio.

Aviso sobre Software Aberto

Este produto inclui código de software desenvolvido por terceiros, incluindo código de software sujeito à GNU General Public License (GPL) ou GNU Lesser General Public License (LGPL). Conforme o caso, os termos de GPL e LGPL, e as informações sobre como obter acesso ao código GPL e LGPL usados neste produto, estão disponíveis para você em http://192.168.0-1/GPL/ (incluindo RG web UI).

O código GPL e LGPL usado neste produto é distribuído SEM QUALQUER GARANTIA e está sujeito a direitos autorais de um ou mais autores. Para mais detalhes, consulte o Código GPL e LGPL para este produto e os termos de GPL e LGPL.