

Cuidados e Segurança

Tratamento de dados

- » Este sistema utiliza e processa dados pessoais, como senhas, endereços de rede e registro dos dados de clientes.
- » LGPD - Lei Geral de Proteção de Dados Pessoais: este produto faz tratamento de dados pessoais, porém a Intelbras não possui acesso aos dados a partir deste produto. Este produto possui criptografia na transmissão e armazenamento dos dados pessoais.

Proteção e segurança de dados

- » Observar as leis locais relativas à proteção e uso de dados e as regulamentações que prevalecem no país.
- » O objetivo da legislação de proteção de dados é evitar infrações nos direitos individuais de privacidade, baseadas no mau uso dos dados pessoais.

Diretrizes que se aplicam aos funcionários da Intelbras

- » Os funcionários da Intelbras devem cumprir com as práticas de comércio seguro e confidencialidade de dados sob os termos dos procedimentos de trabalho da companhia.
- » É imperativo que as regras a seguir, sejam observadas para assegurar que as provisões estatutárias relacionadas a serviços (sejam serviços internos ou de administração e manutenção remota) sejam estritamente seguidas. Isso preserva os interesses do cliente e oferece proteção pessoal adicional.

Diretrizes que controlam o tratamento de dados

- » Assegurar que apenas pessoas autorizadas tenham acesso aos dados de clientes.
- » Usar as facilidades de atribuição de senhas, sem permitir qualquer exceção. Jamais informar senhas para pessoas não autorizadas.
- » Assegurar que nenhuma pessoa, não autorizada, tenha como processar (armazenar, alterar, transmitir, desabilitar ou apagar) ou usar dados de clientes.
- » Evitar que pessoas, não autorizadas, tenham acesso aos meios de dados, por exemplo, discos de backup ou impressões de protocolos.
- » Assegurar que os meios de dados que não são mais necessários, sejam completamente destruídos e que documentos não sejam armazenados ou deixados em locais geralmente acessíveis.
- » O trabalho em conjunto com o cliente gera confiança.
- » Este produto possui criptografia na transmissão dos dados pessoais.

Uso indevido e invasão de hackers

- » As senhas de acesso às informações do produto, permitem o alcance e a alteração de qualquer facilidade, como o acesso externo ao sistema da empresa para obtenção de dados, portanto, é de suma importância que as senhas sejam disponibilizadas apenas àqueles que tenham autorização para uso, sob o risco de uso indevido.
- » O produto possui configurações de segurança que podem ser habilitadas, e que serão abordadas neste manual, todavia, é imprescindível que o usuário garanta a segurança da rede na qual o produto está instalado, haja vista que o fabricante não se responsabiliza pela invasão do produto via ataques de hackers e crackers.



ATENÇÃO:

Este produto vem com uma senha-padrão de fábrica. Para sua segurança, é IMPRESCINDÍVEL que você a troque assim que instalar o produto e questione o seu técnico quanto as senhas configuradas, quais os usuários que possuem acesso e os métodos de recuperação.



ATENÇÃO:

Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados.

Este é um produto homologado pela Anatel, o número de homologação se encontra na etiqueta do produto, para consultas acesse o site: sistemas.anatel.gov.br/sch.

Acesso ao equipamento

Primeiro acesso

O produto pode ser acessado através da interface de gerenciamento web do equipamento. Execute o procedimento a seguir para acessar seu equipamento:

1. Conecte um cabo de rede entre seu computador e o equipamento;
2. Certifique-se de que seu computador se encontra na mesma rede que o equipamento, **ex. 10.0.0.2/24**;
 - » Acesse as configurações de rede de seu computador.

» dentro da interface que o equipamento estiver conectado (por padrão Ethernet), configure o IPv4 como fixo. **Endereço IP: 10.0.0.2 e máscara de sub-rede: 255.255.0.0**

Obs.: É possível fazer realizar um ping para o equipamento via terminal para verificar que a configuração foi feita com sucesso.

3. Digite o endereço **10.0.0.1** na barra de endereço do navegador;
4. Se tiver êxito no acesso, a tela de login da imagem abaixo será exibida:

Entrar

Idioma

 Português ▼

Usuário

 Nome do usuário

Senha

 Digite sua senha 

ENTRAR

Insira as seguintes informações:

- » **Usuário:** admin
- » **Senha:** A senha padrão do equipamento é aleatória e pode ser encontrada na etiqueta do produto, como verificado na imagem abaixo.

IP Fallback: 10.0.0.1
Alimentação: 48V/0,5A ou 802.3at
Usuário: admin
Senha produto: XXXXXXXX
Senha Wi-fi: XXXXXXXXXXXX

Obs.: o idioma português é pré-definido por padrão e pode ser alterado.

A página de primeiro acesso será exibida:


Primeiro acesso

Por motivos de segurança, altere a senha para acessar o equipamento.

Idioma

 Português

Usuário

 admin

Senha





Senha deve ter de 8 a 63 caracteres;
Conter pelo menos 1 (um) número;
Conter pelo menos 1 (uma) letra maiúscula;
Conter pelo menos 1 (uma) letra minúscula;
Conter pelo menos 1 (um) caractere especial (Ex: #, *, !, @).

Confirmar senha





☒ Li e concordo com a [Política de Privacidade](#) e os [Termos de Uso](#)

ENTRAR

Intelbras © 2023 - [Privacidade](#) - [Termos](#)

Digite uma nova senha de usuário com no mínimo 8 caracteres e máximo de 63 caracteres, contendo:

- » Pelo menos 1 (um) número;
- » Pelo menos 1 (uma) letra maiúscula;
- » Pelo menos 1 (uma) letra minúscula;
- » Pelo menos 1 (um) caractere especial dentre os seguintes \$(| ~ \ ^ ` : ; < = > ? @ ! " # \$ % & ' () * + , . { } [] _ - /).

Clique em entrar Senha.

Então o equipamento apresentará a tela inicial Dashboard e estará pronto para iniciar as configurações de uso.

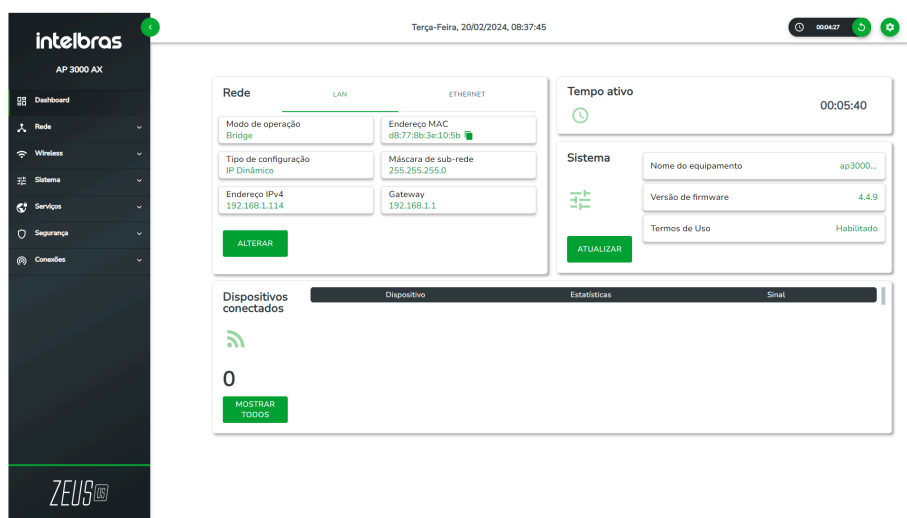
Obs.: o produto da Intelbras vem com o padrão IP 10.0.0.1. Contudo, receberá um novo endereço IP, se for inserido em uma rede com DHCP, de acordo com a faixa configurada no servidor DHCP. Para consultar o IP obtido, verifique no seu servidor DHCP. Caso queira apenas acessar a interface do produto, basta digitar meu.intelbras no seu navegador em um computador na mesma rede do AP. Após o primeiro acesso, utilizar o login admin e nova senha cadastrada.

Caso você se esqueça da senha, é possível resetar o equipamento e configurá-lo novamente. Consulte a seção [Reset \(padrão de fábrica\)](#) para entender os

procedimentos de reset físico e reset via software.

Interface e informações gerais


Ao acessar o equipamento, a tela de Dashboard é apresentada:

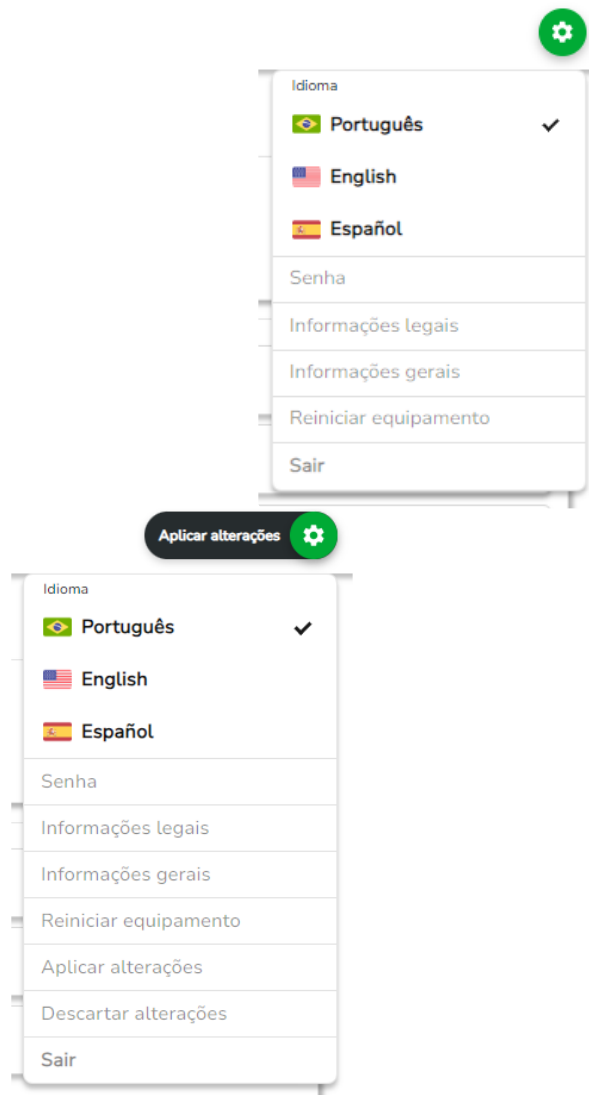


Menu lateral

- » **Dashboard:** Permite acessar o dashboard do equipamento.
- » **Rede:** Permite alterar o modo de operação e o configurar o comportamento da rede do equipamento
- » **Wireless:** Permite gerenciar as redes wireless criadas pelo equipamento e o comportamento delas. Também permite consultar redes Wi-Fi próximas e autenticação de servidor radius
- » **Sistema:** Permite acessar configurações de sistema do equipamento, aplicar reset ao padrão de fábrica, realizar uma atualização, entre outras.
- » **Serviços:** Permite configurar os serviços disponíveis no equipamento, como Splash Page, Discovery, DDNS, etc.
- » **Segurança:** Permite configurar o funcionamento das medidas de segurança do firewall do equipamento.
- » **Conexões:** Permite verificar informações sobre os clientes conectados nas interfaces do equipamento.

Menu suspenso

Ao clicar no botão  no canto superior direito, o menu suspenso será exibido:

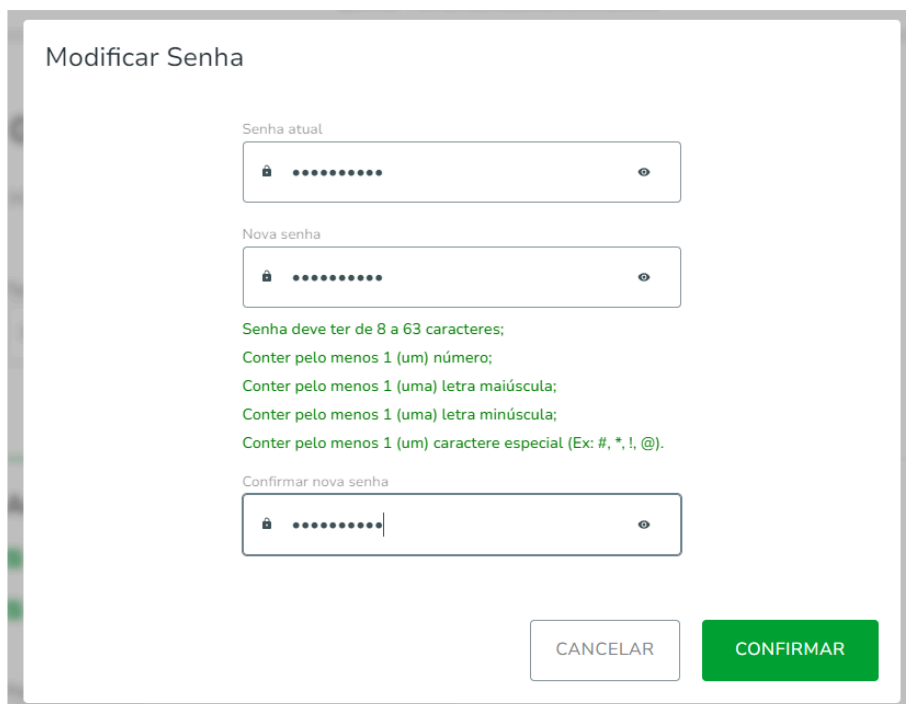


Obs.: O menu suspenso com "Aplicar alteração" e "Descartar alteração" somente são apresentados ao ter alterações salvas pendentes.

A partir dele é possível ter acesso à escolha de idioma, alteração de senha, informações legais e gerais, bem como aplicar/descartar as alterações, reiniciar o equipamento ou finalizar a sessão.

Senha:

Use essa funcionalidade para trocar a senha de administração de tempos em tempos.



Modificar Senha

Senha atual

Nova senha

Senha deve ter de 8 a 63 caracteres;
 Conter pelo menos 1 (um) número;
 Conter pelo menos 1 (uma) letra maiúscula;
 Conter pelo menos 1 (uma) letra minúscula;
 Conter pelo menos 1 (um) caractere especial (Ex: #, *, !, @).

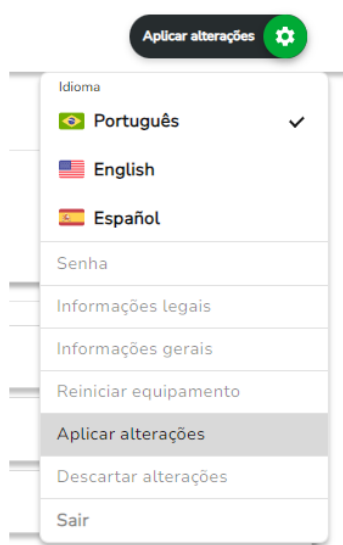
Confirmar nova senha

CANCELAR CONFIRMAR

- » **Senha atual:** digite a senha atual de administração.
- » **Nova senha:** digite a nova senha de administração.
 - » Mínimo 8 caracteres e máximo de 63 caracteres;
 - » Pelo menos 1 (um) número;
 - » Pelo menos 1 (uma) letra maiúscula;
 - » Pelo menos 1 (uma) letra minúscula;
 - » Pelo menos 1 (um) caractere especial dentre os seguintes \$(| ~ \ ^ ` : ; < = > ? @ ! " # \$ % & ' () * + , . { } [] _ - /).
- » **Confirmar nova senha:** digite novamente a nova senha de administração.

Aplicar ou descartar alterações:

Ao clicar em Aplicar ou Descartar Alterações, será solicitada confirmação adicional como nas imagens abaixo:



Obs.: Ao clicar em "Confirmar alteração", o equipamento irá reiniciar com as últimas configurações salvas.

Aplicar alterações

Todas as informações serão substituídas e o equipamento pode ser reiniciado após a finalização do processo. Tem certeza que deseja continuar?

ou

Descartar alterações

Há configurações que não foram aplicadas. Deseja descartá-las agora?

Reiniciar Equipamento:

Permite ao administrador realizar reboot do equipamento.

Reiniciar equipamento

Caso possua alterações a serem aplicadas, as mesmas serão descartadas. Tem certeza que deseja reiniciar o equipamento?

Informações Legais:

É possível visualizar a Política e Privacidade e os Termos de uso.

Política e Privacidade

Política de Privacidade

POLÍTICA DE PRIVACIDADE Versão atualizada em 06.01.2020 1. Informações Importantes 1.1. No decorrer dessa política, adotamos os termos abaixo listado com os respectivos significados: • Autoridade Nacional de Proteção de Dados (ANPD) - É o órgão que fiscalizará e orientará a aplicação da LGPD, bem como é responsável pela aplicação de sanções administrativas em caso de violação à lei. • Base Legal para Tratamento - O tratamento de Dados Pessoais é permitido pela LGPD de acordo com as bases legais previstas, tais como o consentimento do Titular, o cumprimento de obrigações legais e/ou regulatórias pela Intelbras, a existência de contrato entre a Intelbras e o Titular, análise para proteção ao crédito, bem como legítimos interesses da Intelbras ou do Titular. • Biometria - Uma característica física mensurável ou um traço pessoal comportamental pessoal usado para reconhecer ou verificar a identidade de uma pessoa. Imagens faciais, impressões digitais e amostras de íris são exemplos de biometria. • Comitê de Privacidade - Significa o comitê de pessoas da Intelbras composto por representantes do Departamento Jurídico, TI e Qualidade, responsável pela representação da Intelbras perante os titulares e a ANPD, bem como será



Li e concordo com a Política de Privacidade.

FECHAR

Termos de uso:

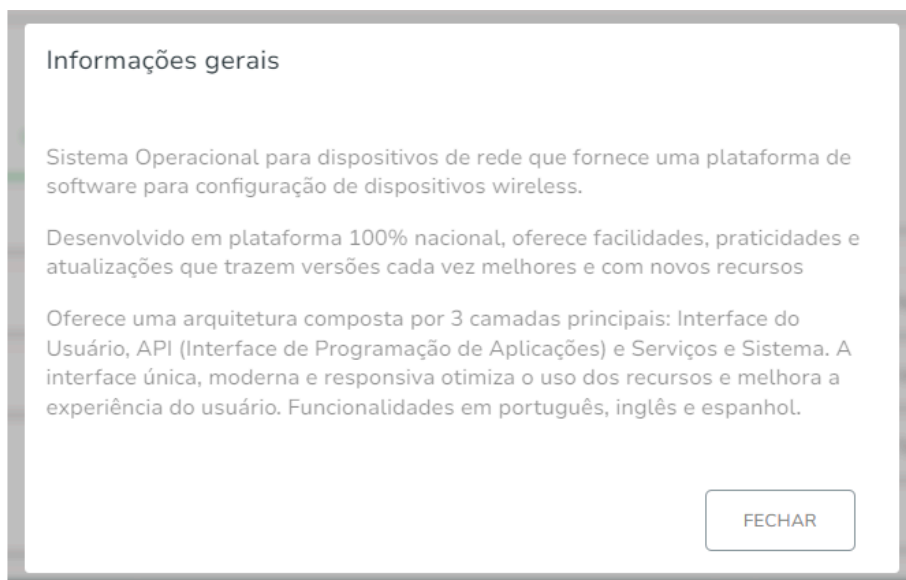
Termos de Uso

Termos de Uso INTELBRAS Versão atualizada em 06.01.2020 Para utilizar o AP 1750 AC, é indispensável a aceitação dos termos descritos a seguir. Estes Termos de Uso de Produto (CONTRATO) é um acordo legal entre o USUÁRIO (pessoa física ou jurídica), denominado USUÁRIO, e a INTELBRAS S/A - Indústria de Telecomunicação Eletrônica Brasileira, pessoa jurídica de direito privado, inscrita no CNPJ sob n.º 82.901.000/0001-27, estabelecida à rodovia BR 101, km 210, Área Industrial, São José - SC, doravante denominada INTELBRAS, para uso do AP 1750 AC, podendo incluir os meios físicos associados, bem como quaisquer materiais impressos e qualquer documentação online ou eletrônica. Ao utilizar o PRODUTO, mesmo que parcialmente ou a título de teste, o USUÁRIO estará vinculado aos termos deste contrato, concordando com suas disposições, principalmente com relação ao consentimento para o acesso, coleta, uso, armazenamento, tratamento e técnicas de proteção às informações do USUÁRIO pela INTELBRAS, necessárias para a integral execução das funcionalidades ofertadas pelo PRODUTO. Em caso de discordância com os termos aqui apresentados, a utilização do PRODUTO deve ser imediatamente

FECHAR

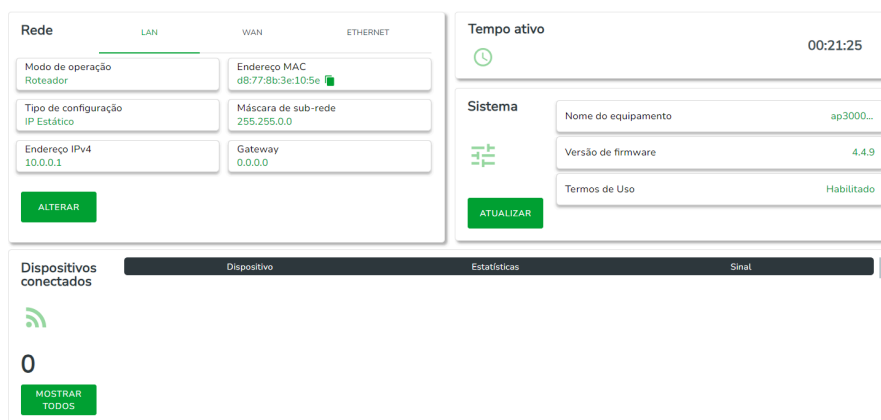
Informações Gerais:

Também é possível pelo menu suspenso ter acesso às informações gerais do sistema.



Dashboard

Dashboard



- » **Rede:** Permite visualizar informações e alterar o comportamento da rede. Configurações de rede local (LAN), configurações de rede remota (WAN), Ethernet e Modo de operação
- » **Tempo ativo:** Permite visualizar o tempo total de operação do equipamento desde que foi ligado.
- » **Sistema:** Permite visualizar detalhes sobre o equipamento, como nome, versão do firmware e termos de uso. É possível acessar as configurações de sistema pelo menu lateral.

- » **Equipamentos conectados:** Permite visualizar a lista dos clientes conectados ao equipamento, como suas estatísticas e sinais.

Rede

Modo de operação

Permite definir o comportamento do equipamento na rede.

| Modo de operação

Nome do equipamento

ap3000ax

Modo de operação

Roteador



Habilitar NAT

Salvar

- » **Nome do equipamento:** nome/apelido que pode ser configurado para cada equipamento na rede, com o intuito de facilitar sua identificação.
- » **Modo de operação:**
 - Bridge:** o equipamento opera como uma ponte entre os clientes conectados e as interfaces externas, mantendo a comunicação na mesma rede.
 - Roteador:** o equipamento faz o roteamento entre os clientes conectados e as interfaces externas, gerando uma sub-rede para os clientes conectados.
- » **Habilitar NAT:** habilita a operação do NAT na interface de rede do produto.

WAN

Permite configurar parâmetros relacionados à conexão do equipamento com a internet (WAN).

Obs.: essa funcionalidade está disponível apenas quando o modo de operação for Roteador.

IPv4

Tipo de configuração:

PPPoE: escolha PPPoE para conectar ao seu provedor de acesso via PPPoE.

WAN

IPv4

Tipo de configuração

PPPoE

☐ Clonar endereço MAC

☐ MPPE

Nome do serviço

Usuário

Senha

MTU

1492

☐ VLAN

Salvar

- » **MPPE:** habilita criptografia MPPE (Microsoft Point-to-Point Encryption).
- » **Nome do serviço:** nome do serviço PPPoE de seu provedor.
- » **Usuário PPPoE:** define o nome do usuário para autenticação PPPoE.
- » **Senha:** define a senha para autenticação PPPoE.

IP estático: define as configurações de IP manualmente.

WAN

Configuração de Rede Local

IPV4

IPV6

Tipo de Configuração

IP Estático

☐ Clonar Mac

Clonar endereço MAC da WAN

d8:77:8b:3e:10:5b

Endereço IPv4

192.168.0.1

Máscara de Sub-rede

Informe no formato CIDR, ex: 16

24

Gateway

192.168.0.254

MTU

1500

*O MTU deve ser alterado somente se for necessário. O valor máximo de MTU é 1500

☒ VLAN

SALVAR

- » **Clonar MAC:** define um endereço MAC a ser clonado. Alguns provedores restringem o acesso a um endereço MAC previamente detectado por outro equipamento. Assim sendo, você deve notificar seu provedor quanto à troca de MAC ou simplesmente clonar o MAC do equipamento anterior.
- » **Endereço IPv4:** define o endereço IP da interface.
- » **Máscara de Sub-rede:** define a máscara de sub-rede da interface.
- » **Gateway:** define o gateway-padrão da interface.
- » **MTU (Maximum Transmission Unit):** é o tamanho máximo do pacote que a interface pode transmitir.
- » **VLAN:** possibilita acessar a interface WAN a partir de uma rede virtual local, atribuindo um VLAN ID para esta interface.
- » **Cliente DHCP:** define a WAN para receber um endereço IP automaticamente por um servidor DHCP.

WAN

Configuração de Rede Local

IPV4

IPV6

Tipo de Configuração

Cliente DHCP

☐

 Clonar Mac

Clonar endereço MAC da WAN

d8:77:8b:3e:10:5b

MTU

1500

*O MTU deve ser alterado somente se for necessário. O valor máximo de MTU é 1500

☐

 VLAN

SALVAR

IPv6

Tipo de configuração:

» **Desabilitado:** desabilitar o endereço IPv6 no equipamento.

WAN

Configuração de Rede Local

IPV4

IPV6

Tipo de Configuração

Desabilitado

SALVAR

» **IP Estático:** o endereço do IPv6 deve ser especificado manualmente.

WAN

Configuração de Rede Local

IPV4

IPV6

Link-local:
Salve e aplique as alterações para que o link local apareça.

Tipo de Configuração
IP Estático

Endereço IPv6

Tamanho do prefixo

Gateway
::

SALVAR

»

- » **Endereço IP:** especifica o endereço IPv6 para a interface.
- » **Tamanho do prefixo:** insere o comprimento do prefixo IPv6 para o endereço.
- » **Gateway:** especifica o endereço do IPv6 para o gateway padrão.
- » **Automático:** IP gerado automaticamente pelo produto. Pode operar no modo Stateless ou Stateful.

WAN

Configuração de Rede Local

IPV4

IPV6

Link-Local
fe80::da36:5fff:fed8:f1a8/64

Tipo de Configuração
Automático

SALVAR

- » **Link local:** IP gerado automaticamente pelo produto.

WAN

Configuração de Rede Local

IPV4

IPV6

Link-Local

fe80::da36:5fff:fed8:f1a8/64

Tipo de Configuração

Link-Local

SALVAR

LAN

Permite configurar parâmetros relacionados à conexão do equipamento com a rede local (LAN).

Caso seu equipamento esteja em modo de operação Bridge, a seguinte tela será apresentada. IPv4

LAN

Configuração da Rede Local

IPV4

IPV6

☒ Endereço IP dinâmico (automático) ⓘ

Endereço de IP fixo / fallback

10.0.0.1

Máscara de sub-rede

Informe no formato CIDR, ex: 16

16

Gateway padrão

10.0.255.254

SALVAR

- » **Endereço IP dinâmico (automático):** marque para obter endereço de um servidor DHCP.
- » **Endereço de IP Fixo / Fallback:** endereço a ser atribuído, caso o equipamento não receba corretamente o endereçamento, através do servidor DHCP.
- » **Máscara de Sub-rede:** máscara de sub-rede do equipamento.

» **Gateway Padrão:** define o gateway-padrão da interface.

Para equipamentos configurados em modo de operação Roteador, a seguinte tela será apresentada.

The screenshot shows the 'LAN' configuration page with the subtitle 'Configuração da Rede Local'. It features two tabs: 'IPV4' (active) and 'IPV6'. Under the 'IPV4' tab, there are two input fields: 'Endereço de IP Fixo' containing '10.0.0.1' and 'Máscara de sub-rede' containing '16'. Below these fields is a green 'SALVAR' button.

» **Endereço de IP Fixo / Fallback:** endereço a ser atribuído, caso o equipamento não receba corretamente o endereçamento, através do servidor DHCP.

» **Máscara de Sub-rede:** máscara de sub-rede do equipamento.

IPv6

» **Tipo de configuração:**

» **Automático:** IP gerado automaticamente pelo produto. Pode operar no modo Stateless ou Stateful.

The screenshot shows the 'LAN' configuration page with the subtitle 'Configuração da Rede Local'. It features two tabs: 'IPV4' and 'IPV6' (active). Under the 'IPV6' tab, there is a dropdown menu labeled 'Tipo de Configuração' with 'Automático' selected. Below this is a green 'SALVAR' button.

» **Desabilitado:** desabilitar o endereço IPv6 no equipamento.

LAN

Configuração da Rede Local

IPV4

IPV6

Link-Local

Desabilitado

Tipo de Configuração

Desativado

SALVAR

» **Link local:** IP gerado automaticamente pelo produto.

LAN

Configuração da Rede Local

IPV4

IPV6

Link-Local

fe80::da36:5fff:fed8:f1aa/64

Tipo de Configuração

Link-Local

SALVAR

» **Manual:** o endereço do IPv6 deve ser especificado manualmente.

LAN

Configuração da Rede Local

IPV4

IPV6

Tipo de configuração

Manual

Link - Local:

fe80::da77:8bff:fe3e:105b/64

Endereço IP

Tamanho do prefixo

Gateway padrão

SALVAR

- » **Endereço IP:** especifica o endereço IPv6 para a interface.
- » **Tamanho do Prefixo:** insere o comprimento do prefixo IPv6 para o endereço.
- » **Gateway Padrão:** especifica o endereço do IPv6 para o gateway padrão. **Obs.:** disponível somente para o modo bridge.

DHCP

Permite configurar um servidor DHCP na sua rede, como também definir um IP estático.

Rede DHCP

Configuração de DHCP (Dynamic Host Configuration Protocol) que permite ao dispositivo obter automaticamente um endereço IP e outras informações relacionadas.

IPv4



Habilitar DHCP



Proteção contra ataque DNS Rebind

Endereço IP Inicial

10.0.0.2

Endereço IP Final

10.0.255.254

Tempo de Renovação

1800



Adicionar

Habilitado	Descrição	IP	MAC
Nenhum DHCP Estático cadastrado.			

SALVAR

- » **Habilitar DHCP:** permite habilitar ou desabilitar o servidor DHCP.
- » **Proteção contra ataque de DNS Rebind:** permite desativar DNS Rebind.
- » **Endereço IP Inicial:** permite definir o IP inicial do intervalo dos possíveis endereços IP da rede.
- » **Endereço IP Final:** permite definir o IP final do intervalo dos possíveis endereços IP da rede.
- » **Tempo de Renovação:** controla o tempo de renovação dos endereços, indicando o tempo em que o servidor verifica se os clientes estão ativos.

Obs.: ao desabilitar esta função você pode ser vítima de ataques, do tipo spam, ataques distribuídos de negação de serviço (DDoS) e outras atividades maliciosas.

Configurando um IP estático na rede:

- » Clique em Adicionar.
- » Preencha as informações do equipamento: IP, MAC e Descrição.
- » Clique em Adicionar.

Obs.: a quantidade máxima de IPs estáticos possíveis é igual a quantidade de IPs configurados na opção Intervalo do Servidor DHCP.

DNS

Permite selecionar se os endereços dos servidores DNS serão definidos automaticamente ou manualmente.

IPv4

» **Modo DNS:**

» **DNS manual:** permite que os servidores DNS sejam definidos manualmente.

Rede DNS

Configuração de Servidor

IPv4

IPv6

Modo DNS

Modo Manual

Servidor DNS primário

8.8.8.8

Servidor DNS secundário

8.8.4.4

SALVAR

» **Servidor DNS 1:** define o endereço IP do servidor DNS primário.

» **Servidor DNS 2:** define o endereço IP do servidor DNS secundário.

» **DNS automático:** permite que os servidores DNS sejam definidos automaticamente.

Rede DNS

Configuração de Servidor

IPv4

IPv6

Modo DNS

Modo Automático

Servidor DNS primário

8.8.8.8

Servidor DNS secundário

8.8.4.4

SALVAR

IPv6

» Modo DNS:

» **DNS manual:** permite que os servidores DNS sejam definidos manualmente.

Rede DNS

Configuração de Servidor

IPV4

IPV6

Modo DNS

Modo Manual

Servidor DNS primário

2001:4860:4860::8888

Servidor DNS secundário

2001:4860:4860::8844

SALVAR

» **Servidor DNS 1:** define o endereço IP do servidor DNS primário.

» **Servidor DNS 2:** define o endereço IP do servidor DNS secundário.

» **DNS automático:** permite que os servidores DNS sejam definidos automaticamente.

Rede DNS

Configuração de Servidor

IPV4

IPV6

Modo DNS

Modo Automático

Servidor DNS primário

2001:4860:4860::8888

Servidor DNS secundário

2001:4860:4860::8844

SALVAR

Captive Portal

Configuração de autenticação externa de usuários na rede.

Captive portal

Configuração de autenticação externa de usuários na rede

Lista de SSID

Habilitado	SSID	Frequência	Tipo de Autenticação
<input type="checkbox"/>	AP3000AX_f1a8	Dual band	WPA2-PSK

Configuração Externa

Endereço de Captive Portal Externo (autenticador)

https://

Tempo de Sessão ⓘ

30 minutos

Tempo de inatividade ⓘ

5 minutos


Tipo de Autenticação

Externo

Senha

Walled Garden ⓘ

 ADICIONAR

Endereço

Excluir

Salvar

- » **Habilitar Captive Portal:** selecione as redes Wi-Fi que utilizarão a função Captive Portal.
- » **Endereço do Captive Portal Externo (autenticador):** endereço da página externa na qual o usuário será redirecionado para autenticação.
- » **Tempo de sessão:** tempo de sessão do usuário. Ao expirar o tempo configurado, a sessão será encerrada e o usuário precisará se re-autenticar. O tempo de sessão informado acima só será aplicado quando um intervalo válido não for definido pelo servidor. Pode ser definido em minutos, horas ou dias.
- » **Tempo de inatividade:** ao ser detectada a inatividade do usuário no limite configurado, o mesmo terá sua sessão encerrada. Pode ser definido em minutos, horas ou dias.
- » **Tipo de autenticação:** Externo ou Radius.
- » **Externo:** permite definir a senha utilizada pelo AP para autenticar-se no servidor captive portal externo.
- » **Radius:** permite definir qual dos servidores Radius cadastrados deve ser usado para autenticação.

Tipo de Autenticação

Radius


 ADICIONAR

Servidor	Endereço do Servidor	Porta Authentication	Porta Accounting
Servidor Exemplo	10.0.0.1	1812	1813

» Walled Garden

O Zeus OS permite adicionar outros domínios para acesso antes de se autenticar ao Captive Portal Externo através do Walled Garden. Se necessário acessar outro domínio antes da autenticação, é necessário adicionar nessa opção.

Walled Garden ⓘ

 ADICIONAR

Endereço
<input type="text" value="https://"/>

QoS

Utilize a opção QoS para limitar/garantir a banda por SSID ou para limitar a banda por IP/MAC.

QoS

Controle o tráfego do dispositivo, classificando, priorizando ou limitando.

☐ Habilitar QoS

Tipo de QoS

Limite/Garantia de Banda por SSID ▼

Link da Internet

Upload (Mbps)

1000

Download (Mbps)

1000

Limite de Banda por SSID

Habilitado	SSID	Frequência	Upload (Mbps)	Download (Mbps)
<input type="checkbox"/>	AP3000AX_f1a8	Dual band	1000	1000

Garantia de Banda por SSID ⓘ

Habilitado	SSID	Frequência	Upload (%)	Download (%)
<input type="checkbox"/>	AP3000AX_f1a8	Dual band	1	1

Salvar

Link da internet

Link da Internet

Upload (Mbps)

Download (Mbps)

- » **Upload (Mbps):** Informe a velocidade real de upload do link de internet (para fins de cálculo percentual).
- » **Download (Mbps):** Informe a velocidade real de download do link de internet (para fins de cálculo percentual).

Obs.: A taxa de transferência máxima do produto pode ser afetada ao ativar a função QoS.

Limite de banda por IP/MAC

Obs.: A funcionalidade Limite de Banda por IP/MAC está disponível apenas em modo Roteador.

+ Adicionar

Habilitado	Descrição	IP / Rede	MAC	Upload (Mbps)	Download (Mbps)
<input checked="" type="checkbox"/>	Exemplo	<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text" value="1"/>

- » **Habilitado:** Selecione para habilitar a opção de limite de banda.
- » **Descrição:** Descrição da limitação.
- » **Rede/IP:** Rede/IP cuja banda deseja limitar.
- » **MAC:** Endereço MAC do equipamento.
- » **Upload (Mbps):** Informe o valor em Mbps, para limitar banda de upload, para o SSID correspondente.
- » **Download (Mbps):** Informe o valor em Mbps, para limitar banda de download, para o SSID correspondente.

Limite de banda por SSID

Limite de Banda por SSID

Habilitado	SSID	Frequência	Upload (Mbps)	Download (Mbps)
<input type="checkbox"/>	AP3000AX_f1a8	Dual band	<input type="text" value="1000"/>	<input type="text" value="1000"/>

- » **Habilitado:** Selecione para habilitar a opção de limite de banda.
- » **SSID:** SSID da rede.
- » **Frequência:** Em qual/quais frequências o SSID está atuando na rede.
- » **Upload (Mbps):** Informe o valor em Mbps, para limitar banda de upload, para o SSID correspondente.
- » **Download (Mbps):** Informe o valor em Mbps, para limitar banda de download, para o SSID correspondente.

Garantia de banda por SSID

Garantia de Banda por SSID ¹

Habilitado	SSID	Frequência	Upload (%)	Download (%)
<input type="checkbox"/>	AP3000AX_f1a8	Dual band	1	1

- » **Habilitado:** Marque para ativar o controle de garantia de banda.
- » **SSID:** SSID da rede.
- » **Frequência:** Em qual/quais frequências o SSID está atuando na rede.
- » **Upload (Mbps):** Porcentagem de banda de upload configurada no link da internet, garantida para a rede sem fio selecionada.
O cálculo da porcentagem não pode resultar em valor menor que 0,001Mbps.
Para redes "Dual band", o valor da porcentagem é dividido entre as duas frequências (2.4GHz e 5GHz).
- » **Download (Mbps):** Porcentagem de banda de upload configurada no link da internet, garantida para a rede sem fio selecionada.
O cálculo da porcentagem não pode resultar em valor menor que 0,001Mbps.
Para redes "Dual band", o valor da porcentagem é dividido entre as duas frequências (2.4GHz e 5GHz).

Obs.: É recomendado não aplicar mais de 256 regras para limite de banda.

Rotas

Permite criar ou excluir rotas na tabela de roteamento do equipamento.

Obs.: Essa funcionalidade está disponível apenas quando o modo de operação for Roteador.

Rotas

Permite a conexão de grupos de computadores entre diferentes redes IPv4.

IPv4

Descrição

Rota de destino



Gateway

+ CRIAR ROTA

Rotas criadas

Exemplo

Rota de destino: 10.0.0.0/32 Gateway: 192.168.0.0

SALVAR

- » **Descrição:** Insira uma descrição para a rota a ser criada.

- » **Rede de destino:** Define a rede destino/máscara.
- » **Máscara de Sub-Rede:** Máscara de sub-rede do equipamento para a rota específica.
- » **Gateway:** Define o gateway-padrão de destino para essa rota.

Use o botão **+** Adicionar para criar as rotas e preencher a tabela de roteamento, ou use o botão **🗑** para excluir uma rota.

Wireless

Wireless

Permite definir o comportamento do equipamento nas redes sem fio.



- » Ao clicar em **🗑** Excluir, é possível remover redes wireless cadastradas previamente. Ao clicar em **+** Adicionar ou em **✎** Editar, é possível cadastrar ou editar uma rede wireless pela seguinte tela:

Wireless SSID

Adicionar

Nome da rede (SSID)

Nome da rede (SSID)

Autenticação

Sistema Aberto

☒ Dual band

Configuração avançada

☐ Isolar SSID
 ☐ Somente internet
 ☐ Ocultar SSID
 ☐ Isolar clientes

☒ VLAN

ACL

Modo de controle de acesso

Desabilitado

Máximo de clientes conectados 2.4 GHz

1 128

Máximo de clientes conectados 5 GHz

1 128

Mínimo de sinal do cliente (dBm)

-100 -20

Nome da Rede (SSID): Identificação da rede Wireless.

Caracteres suportados: !, #, \$, %, &, ', (,), *, +, ,, -, ., /, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, :, ;, <, =, >, ?, @, A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, [, \,], ^, _ , ` , a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z, {, |, }, ~

Tipo de autenticação:

- » **Sistema Aberto:** Autenticação desabilitada.
- » **WPA:** Tipo de autenticação baseado em IEEE 802.11, utilizando criptografia AES ou TKIP/AES (requer servidor RADIUS).
 - » **Senha:** Senha do servidor RADIUS.
 - » **Criptografia:** AES ou TKIP/AES.
 - » **NAS ID:** ID de identificação para o servidor Radius.
 - » **Porta:** Porta do servidor RADIUS.
 - » **Server address:** Endereço do servidor RADIUS.
- » **WPA2:** Tipo de autenticação baseado em IEEE 802.11, utilizando criptografia AES ou TKIP/AES (requer servidor RADIUS).
 - » **Senha:** Senha do servidor RADIUS.
 - » **Criptografia:** AES ou TKIP/AES.
 - » **NAS ID:** ID de identificação para o servidor Radius.
 - » **Porta:** Porta do servidor RADIUS.
 - » **Server address:** Endereço do servidor RADIUS.

- » **WPA-PSK:** Chave pessoal compartilhada, utilizando criptografia AES ou TKIP/AES.
 - » **Criptografia:** AES ou TKIP/AES.
 - » **Senha:** Senha (no mínimo 8 caracteres).
- » **WPA2-PSK:** Chave pessoal compartilhada, utilizando criptografia AES ou TKIP/AES.
 - » **Criptografia:** AES ou TKIP/AES.
 - » **Senha:** Senha (no mínimo 8 caracteres).
- » **Dual Band:** Permite definir o comportamento da rede, se funcionará em modo dual band (2.4 GHz e 5 GHz) ou single band (2.4 GHz ou 5 GHz).
- » **Configuração avançada:**
 - » **Isolar SSID:** Bloqueia a comunicação entre os equipamentos conectados em diferentes SSID.
 - » **Somente internet:** Bloqueia a comunicação entre os clientes conectados neste SSID e o restante da rede local (disponível apenas quando em modo roteador).
 - » **Ocultar SSID:** Permite ocultar a rede sem fio.
 - » **Isolar clientes:** Bloqueia a comunicação entre os equipamentos conectados neste SSID.
 - » **VLAN:** Selecione para habilitar e definir a VLAN.
- » **ACL - Modo do controle de acesso:**
 - » **Desativado:** ACL desativado.
 - » **Permitir listados:** Permite a conexão de clientes definidos na lista de clientes.
 - » **Bloquear listados:** Bloqueia a conexão dos equipamentos adicionados na lista de clientes.
 - » Quando ativado, clique em ➕ Adicionar para incluir clientes na lista.
 - » **Quantidade máxima de registros:** 64
 - » **Máximo de clientes conectados:** Selecione um valor para definir a quantidade de clientes conectados no mesmo SSID.

Obs.: Verifique na ficha técnica do produto a quantidade máxima de clientes suportados.
 - » **Mínimo de sinal do cliente (dBm):** Permite configurar o valor mínimo de sinal aceitável de cada cliente conectado.

Wireless avançado

Permite definir configurações e funcionalidades extras da interface Wireless.

Wireless Avançado

Funcionalidades extras da interface Wireless

Wireless Roaming ⓘ

☒ Habilitar Assisted Roaming (802.11k e 802.11v) ☐ Habilitar Fast Roaming (802.11r)

Smart Handover ⓘ

☐ Habilitar Smart Handover

☐ Definir este AP como principal

Certifique-se que apenas um AP esteja configurado como principal

Band Steering ⓘ

☒ Habilitar

Método

Balanceamento de clientes entre frequências ▾

Beamforming ⓘ

☒ Habilitar

- » **Wireless Roaming:** permite que os clientes conectados transitem de um AP para o outro de forma transparente e sem perda de pacotes.
- » **Habilitar Assisted Roaming:** suporte aos protocolos 802.11k e 802.11v. Marque para habilitar a função em seu equipamento. Com a função habilitada, o AP irá sugerir a transição para os equipamentos quando for conveniente.
- » **Habilitar Fast Roaming:** suporte ao protocolo 802.11r. Marque para habilitar a função em seu equipamento. Opera somente em SSIDs com criptografia WPA ou WPA2 e requer que o equipamento do cliente tenha suporte a este protocolo.
- » **Smart Handover:** marque para habilitar a função Smart Handover no seu equipamento. Com a função habilitada, o AP irá gerenciar a transição dos equipamentos de forma ativa, com base nas métricas de rede e qualidade do sinal.
- » **Definir este AP como principal:** marque para definir este AP como principal. Os demais APs deverão estar desmarcados e com o mesmo SSID do AP Principal, para correto funcionamento.

Atenção: a funcionalidade Smart Handover é recomendada para redes de pequeno porte, com no máximo 6 roteadores empresariais e 100 equipamentos. Para redes de maior porte, utilize a função Assisted Roaming. O Smart Handover não está disponível para os produtos AX.

Obs.: esta funcionalidade está disponível apenas em Modo de operação Bridge. Verificar na ficha técnica do produto a disponibilidade da função.

- » **Band Steering:** o Band Steering é uma técnica utilizada em ambientes Wi-Fi dual-band que estimula os equipamentos clientes a se conectarem na banda de 5 GHz para

que haja máximo desempenho decorrente da maior capacidade dessa banda, porém a decisão final acerca de qual banda utilizar depende inteiramente do próprio cliente.

Métodos:

- » **Preferencialmente 5 GHz:** realiza a priorização da conexão na rede 5 GHz independente da performance. Se após a conexão, a rede 5 GHz estiver muito degradada (interferência, performance baixa ou muitos clientes conectados consumindo recursos), o usuário será direcionado para a rede 2,4 GHz, pois terá a melhor performance considerada no momento. Se durante o período de conexão deste cliente a rede 5 GHz melhorar a sua performance, o usuário será redirecionado automaticamente para a rede 5 GHz sem perda na conexão.
- » **Balanceamento de clientes entre frequências:** realiza a priorização da conexão baseada na melhor frequência para o usuário. Normalmente a melhor frequência para equipamentos dual band é a de 5GHz. Porém, caso a rede 5 GHz esteja muito degradada (interferência, performance baixa ou muitos clientes conectados consumindo recursos), na conexão, o usuário será direcionado diretamente para a rede 2,4 GHz pois terá a melhor performance considerada no momento. Se durante o período de conexão deste cliente a rede 5 GHz melhorar a sua performance, o usuário será redirecionado automaticamente para a rede 5 GHz sem perda na conexão.

Importante: é muito comum o Balanceamento de clientes entre as frequências falhar por causa da característica de maior alcance do sinal na banda 2,4 GHz, por isso, é muito importante ajustar corretamente a potência do rádio 2,4 GHz, para que ambas as frequências (2,4 GHz e 5 GHz) tenham a mesma potência na prática.

Obs.: a função de Band Steering está disponível apenas para os modelos AP Dual-Band.

- » **Beamforming:** o Beamforming garante que o sinal de Wi-Fi seja direcionado diretamente aos equipamentos dos clientes, evitando perdas durante o processo de transmissão e melhorando o nível de sinal na área de 360° ao redor do AP. Marque para habilitar a função em seu equipamento.

Wireless | Radio 2.4 GHz

Permite definir o comportamento do equipamento nas redes sem fio de 2.4 GHz.

2.4 GHz

Configuração de Rádio

Modo de operação

AP

Modo IEEE

b/g/n

País

Brasil



SITE SURVEY

Largura de Banda

40 MHz

Canal

Automático

SELECIONAR BANDA E CANAL

Potência de Transmissão (dBm) ⁱ

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

SALVAR

- » **Ativar 2.4 GHz:** ativa o funcionamento do equipamento na frequência de 2.4 GHz.
- » **Modo de Operação:** modo de operação do equipamento.
- » **Modo IEEE:** define o padrão de comunicação da rede Wireless.
- » **País:** o país a ser exibido será Brasil.
- » **Canais Suportados:** [Clique aqui](#)
- » **Site survey:** realiza o escaneamento e a listagem e exibição das informações sobre redes sem fio (SSIDs) 2.4 GHz próximas ao dispositivo.

Site Survey 2.4 GHz

ATUALIZAR

Canal	SSID	BSSID	Criptografia	Sinal
7 (2442 MHz)	connect	00:E0:4C:86:70:02		-95 dBm
9 (2452 MHz)	AP3000AX_4859	D8:36:5F:EB:48:5B		-62 dBm
11 (2462 MHz)	AP3000AX_cfac	44:D1:FA:DC:CF:AE		-95 dBm
11 (2462 MHz)	INTELBRAS	D8:77:8B:BF:44:42		-95 dBm
1 (2412 MHz)	Intelbras	D8:77:8B:A9:9C:48		-95 dBm
9 (2452 MHz)	Adolfo	D8:77:8B:05:82:41		-95 dBm
8 (2447 MHz)	1750_router_2g	58:10:8C:8F:57:F9		-33 dBm
9 (2452 MHz)	LUANA	50:02:38:4C:D4:E9		-80 dBm

FECHAR

- » **Canal:** canal utilizado pelo equipamento.
- O botão "Selecionar banda e canal" permite selecionar o canal e a largura de banda:

Seleção de Largura de Banda e Canal

Largura de Banda: 40 MHz

Canal de Extensão: Automático

☐ Preferencialmente a largura selecionada

	Canal	Limite TX, dBm	Largura de Banda Máx.	DFS
<input checked="" type="checkbox"/>	1 (2412 MHz)	24	40	Não
<input checked="" type="checkbox"/>	2 (2417 MHz)	24	40	Não
<input checked="" type="checkbox"/>	3 (2422 MHz)	24	40	Não
<input checked="" type="checkbox"/>	4 (2427 MHz)	24	40	Não
<input checked="" type="checkbox"/>	5 (2432 MHz)	24	40	Não
<input checked="" type="checkbox"/>	6 (2437 MHz)	24	40	Não

FECHAR SELECIONAR

- » **Largura de banda:** o padrão é de 20 MHz para equipamentos baseados no padrão 802.11. Entretanto, os padrões 802.11n, 802.11ac e 802.11ax permitem a junção de canais, aumentando assim a taxa de transferência de dados.
- » **Preferencialmente a largura selecionada:** indica ao AP a preferência em operar na largura selecionada manualmente.
- » **Canal de extensão:** se o padrão for *b/g/n/ax* e a largura de banda 40 MHz, isto define se o segundo canal vai ser acima ou abaixo do canal central.
- » **Seleção de canal:** selecione um canal de preferência. Ao selecionar mais que um canal ou nenhum, a função Canal automático será ativada.
- » **Potência de Transmissão (dBm):** permite especificar manualmente a potência de transmissão.

Wireless | Radio 5 GHz

Permite definir o comportamento do equipamento nas redes sem fio de 5 GHz.

5 GHz

Configuração de Rádio

Modo de operação: AP

Modo IEEE: a/n/ac/ax

País: Brasil

Largura de Banda: 80 MHz

Canal: Automático

SELECIONAR BANDA E CANAL

Potência de Transmissão (dBm) ⓘ

6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

SALVAR

- » **Ativar 5 GHz:** ativa o funcionamento do equipamento na frequência de 5 GHz.

- » **Modo de Operação:** modo de operação do equipamento.
- » **Modo IEEE:** define o padrão de comunicação da rede Wireless.
- » **País:** o país a ser exibido será Brasil.
- » **Canais Suportados:** [Clique aqui](#)
- » **Site survey:** realiza o escaneamento e a listagem e exibição das informações sobre redes sem fio (SSIDs) 5 GHz próximas ao dispositivo.

Site Survey 5 GHz

ATUALIZAR

Canal	SSID	BSSID	Criptografia	Sinal
104 (5520 MHz - DFS)	INTELBRAS-5G	D8:77:8B:BF:44:41		-51 dBm
112 (5560 MHz - DFS)	Neorede_21_A_3	00:1A:3F:69:4F:08		-86 dBm
136 (5680 MHz - DFS)	Neorede_21_Boa_Vista	58:10:8C:17:39:08		-88 dBm
149 (5745 MHz)	GODINHO_5G	24:FD:0D:6D:87:F2		-76 dBm
100 (5500 MHz - DFS)	KARINE_5G	78:17:BE:24:0F:78		-86 dBm
149 (5745 MHz)	Livramento-PLUS	CC:29:BD:5C:93:DA		-87 dBm
149 (5745 MHz)	CITEC_VIVO_5G	84:0B:BB:33:5C:0F		-88 dBm

FECHAR

- » **Canal:** canal utilizado pelo equipamento.

O botão "Selecionar banda e canal" permite selecionar o canal e a largura de banda:

Seleção de Largura de Banda e Canal

Largura de Banda: 80 MHz

Canal de Extensão: Automático

☐ Preferencialmente a largura selecionada ☐ Mostrar canais com DFS

	Canal	Limite TX, dBm	Largura de Banda Máx.	DFS
<input checked="" type="checkbox"/>	36 (5180 MHz)	14	80	Não
<input checked="" type="checkbox"/>	40 (5200 MHz)	14	80	Não
<input checked="" type="checkbox"/>	44 (5220 MHz)	14	80	Não
<input checked="" type="checkbox"/>	48 (5240 MHz)	14	80	Não
<input checked="" type="checkbox"/>	149 (5745 MHz)	24	80	Não
<input checked="" type="checkbox"/>	153 (5765 MHz)	24	80	Não

FECHAR SELECIONAR

- » **Largura de banda:** o padrão é de 20 MHz para equipamentos baseados no padrão 802.11. Entretanto, os padrões 802.11n, 802.11ac e 802.11ax permitem a junção de canais, aumentando assim a taxa de transferência de dados.
- » **Preferencialmente a largura selecionada:** indica ao AP a preferência em operar na largura selecionada manualmente.

- » **Canal de extensão:** se o padrão for *a/n/ac/ax* e a largura de banda 80 MHz, isto define se o segundo canal vai ser acima ou abaixo do canal central.
- » **Seleção de canal:** selecione um canal de preferência. Ao selecionar mais que um canal ou nenhum, a função Canal automático será ativada.
- » **Potência de Transmissão (dBm):** permite especificar manualmente a potência de transmissão.
- » **Regra de exibição de autenticação AES/TKIP:**

Wireless	Modos suportados (supported_phy_modes)	Modo IEEE	Largura de Banda Suportada	Criptografia Suportada
2.4 GHz	3	b/g	20 MHz	AES, TKIP/AES
	11	b/g/n	20/40 MHz	AES
	43	b/g/n/AX	20/40 MHz	AES
5 GHz	4	a	20 MHz	AES, TKIP/AES
	12	a/n	20/40 MHz	AES
	28	a/n/ac	20/40/80 MHz	AES
	60	a/n/ac/ax	20/40/80/160 MHz	AES

Site survey

Realiza o escaneamento e a listagem e exibição das informações sobre redes sem fio (SSIDs) próximas ao dispositivo.

Site Survey

Consulta e listagem de redes Wi-Fi próximas.

2.4 GHZ

5 GHZ

 ATUALIZAR

Canal ▲	SSID	BSSID	Criptografia	Sinal
11 (2462 MHz)	INTELBRAS	D8:77:8B:BF:44:42		📶 -55 dBm
11 (2462 MHz)	AP3000AX_cfac	44:D1:FA:DC:CF:AE		📶 -70 dBm
11 (2462 MHz)	CITEB VIVO	84:0B:BB:22:56:08	🔒	📶 -69 dBm
11 (2462 MHz)	Juliane_2.4g	6C:A4:D1:B1:39:70	🔒	📶 -92 dBm
11 (2462 MHz)	intelbras_8B7E	6A:02:71:77:8B:7F	🔒	📶 -60 dBm
11 (2462 MHz)	Miriam	9C:63:5B:54:92:4E	🔒	📶 -85 dBm
11 (2462 MHz)	NO_PONTO	D4:92:5E:F7:F7:AA	🔒	📶 -95 dBm
9 (2452 MHz)	AP3000AX_4859	D8:36:5F:EB:48:5B		📶 -61 dBm
9 (2452 MHz)	LIANA	50:02:38:4C:D4:E9	🔒	📶 -80 dBm

- » O Site Survey pode ser feito dentro das configurações de Wireless rádio ("Radio 5GHz" e "Rádio 2.4GHz"), tendo as informações das redes exibidas de acordo com a configuração do rádio que o usuário se encontra. Ou pode ser feito também no submenu próprio onde o usuário pode selecionar se deseja listar as informações das redes 5GHz ou 2.4GHz.

Radius

Permite configurar servidores Radius no equipamento.

Radius

Autenticação de servidor

NAS ID

 Adicionar

Descrição	Endereço Servidor	Porta Autenticação	Senha
<input type="text" value="Servidor Exemplo"/>	<input type="text" value="10.0.0.1"/>	<input type="text" value="1813"/>	<input type="text" value="12345678"/>

Linhas por página 1 - 1 de 1  

 SALVAR

- » **NAS ID:** ID de identificação para o servidor Radius.
- » **Descrição:** descrição do servidor RADIUS.
- » **Endereço Servidor:** endereço do servidor RADIUS.
- » **Senha:** senha do servidor RADIUS.
- » **Porta Autenticação:** porta do servidor RADIUS.

Sistema

Gerenciamento

HTTP, HTTPS, SSH e VLAN

» Tempo de sessão

Tempo de sessão (segundos) ⓘ

3600

Tempo máximo que o usuário pode ficar sem interagir com o sistema. Quando o usuário ficar inativo, e a contabilização do tempo configurado terminar, a sessão é encerrada e o usuário deve logar novamente para acessar o sistema.

» Acesso HTTP

Gerenciamento de Sistema

HTTP, HTTPS e SSH

Tempo de sessão (segundos) ⓘ

3600

HTTP

HTTPS

SSH

Acesso HTTP

☒ Habilitado

☒ Defesa contra ataque de Força Bruta

☒ Acesso via WAN

Porta padrão: 80

80

SALVAR

» **Acesso via WAN:** habilitar ao equipamento via WAN.

» **Defesa contra ataque de Força Bruta:** ativa a proteção contra ataques de força bruta.

» **Habilitado:** marque para habilitar o acesso via protocolo HTTP.

» **Porta:** informe a porta para aceitar conexões via protocolo HTTP (padrão 80).

» Acesso HTTPS

Gerenciamento de Sistema

HTTP, HTTPS e SSH

Tempo de sessão (segundos) ⓘ

3600

HTTP

HTTPS

SSH

Acesso HTTPS

☒ Acesso via WAN

☒ Defesa contra ataque de Força Bruta

Porta padrão: 443

443

Certificado | Chave

Padrão

Certificado

Buscar

Chave

Buscar

SALVAR

- » **Acesso via WAN:** habilitar ao equipamento via WAN.
- » **Defesa contra ataque de Força Bruta:** ativa a proteção contra ataques de força bruta.
- » **Porta:** informe a porta para aceitar conexões via protocolo HTTPS (padrão 443).
- » **Certificado/chave:** selecione o modo de reconhecimento de certificado/chave HTTPS.
- » **Certificado:** clique em Buscar para localizar o certificado HTTPS a ser utilizado.
- » **Chave:** clique em Buscar para localizar a chave HTTPS a ser utilizada.
- » **Acesso SSH**

Gerenciamento de Sistema

HTTP, HTTPS e SSH

Tempo de sessão (segundos) ⓘ

3600

HTTP

HTTPS

SSH

Acesso SSH

☒ Habilitado

☒ Defesa contra ataque de Força Bruta

☒ Acesso via WAN

Porta padrão: 22

22

SALVAR

- » **Habilitado:** marque para habilitar o acesso SSH ao equipamento.

- » **Defesa contra ataque de Força Bruta:** ativa a proteção contra ataques de força bruta.
- » **Acesso via WAN:** habilitar ao equipamento via WAN.
- » **Certificado/chave:** selecione o modo de reconhecimento de certificado/chave HTTPS.
- » **Porta:** informe a porta para aceitar conexões via protocolo SSH (padrão 22).
- » **Chave:** clique em Buscar para localizar a chave HTTPS a ser utilizada.
- » **VLAN**

Gerenciamento de Sistema

HTTP, HTTPS, SSH e VLAN

Tempo de sessão (segundos) ⓘ

3600

HTTP

HTTPS

SSH

VLAN

VLAN

Interface

Desativado

VLAN de gerência

1

SALVAR

- » **Interface:** permite habilitar a VLAN de gerência na interface Ethernet
- » **VLAN de gerência:** define a VLAN de gerência do equipamento.

Backup e Restauração

Backup e restauração ao padrão de Fábrica.

Backup e Restauração

Backup, Recovery e Padrão de Fábrica.

Realizar backup das configurações

Crie um arquivo de backup com as configurações atuais do equipamento.

CRIAR ARQUIVO DE BACKUP

Aplicar configurações já salvas

Restaurar as configurações salvas à partir de um arquivo de backup

Carregar arquivo

ENVIAR

Restaurar padrão de fábrica

Restaurar as configurações de fábrica do equipamento

RESTAURAR CONFIGURAÇÕES

- » **Criar arquivo de backup:** irá fazer download do arquivo que contém as configurações atuais do produto.
- » **Aplicar configurações já salvas:** permite restaurar as configurações salvas a partir de um arquivo de backup.

Obs.: A restauração do backup deve ser feita a partir de um arquivo gerado da mesma versão do dispositivo que vai ser restaurado "Ex.: backup da versão 4.4.13 restaurado no dispositivo com a versão 4.4.13". Ao realizar a restauração através de arquivos de diferentes versões a **restauração por completo não é garantida**. A restauração entre diferentes versões **não é aconselhada e não deve ser feita**.

- » **Restaurar padrão de fábrica:** redefine as configurações do equipamento ao padrão de fábrica.

Atualização de Firmware

Permite atualizar a versão de firmware do equipamento.

Atualização de Firmware

Versão atual 4.4.9

Seu equipamento está com a última versão disponível: 4.4.9

NOTAS DE VERSÃO

ATUALIZAR

Atualização manual ⓘ

Atualização feita a partir de um arquivo da versão de firmware. Extensão válida: .bin

Selecione a versão de firmware



- » **Atualização automática (via cronos):** caso seja lançada uma versão mais atual o dispositivo ira apresentar uma notificação para que possa atualizar a versão de seu sistema.
- » **Atualização manual:** selecione o arquivo da versão de firmware a ser instalada e clique em "Atualizar". Aguarde até que o processo de atualização seja concluído.

Log

A ferramenta Log de sistema oferece informações de depuração sobre os serviços e protocolos do sistema. Se ocorrer qualquer tipo de mau funcionamento do equipamento, as mensagens aqui registradas, podem ajudar os administradores da rede a identificar e resolver o problema.

Log do Sistema

Registro de ocorrências do sistema

Nível 

Debug



Enviar log para o servidor remoto

Servidor Remoto (FQDN)

Porta padrão: 514

514

SALVAR



ATUALIZAR

Data e Hora	Nível	Mensagem
06/02/2024 - 07:25:54	Depuração	middleware[30202]: "GET /v4/system/log"
06/02/2024 - 07:25:54	Depuração	syslog: Variable "DEFAULT_PASSWORD" not found
06/02/2024 - 07:25:54	Depuração	syslog: Creating storage buffer with 65536 bytes
06/02/2024 - 07:25:54	Depuração	syslog: Calling itb.system.var->get
06/02/2024 - 07:25:54	Depuração	middleware[30198]: "GET /v4/services/log"

Linhas por página 5

1 de 10



EXPORTAR LOG DO SISTEMA

Nível: permite-se selecionar o nível de informação que será exibida no log, sendo:

- » **Nível 3:** Error - error conditions
- » **Nível 4:** Warning - warning conditions
- » **Nível 6:** Info - informational messages
- » **Nível 7:** Debug - debug-level message

Servidor Remoto: é possível enviar as informações do Log do sistema para um servidor remoto de sua preferência. Deve ser informado o nome FQDN (Fully Qualified Domain Name) do servidor e também a porta do servidor. (A porta-padrão é a 514 que envia via protocolo UDP).

Serviços

Splash page

Permite vincular redes sem fio a um vídeo ou imagem da WEB. Ao conectar na rede sem fio, o dispositivo é redirecionado para o conteúdo e a visualização é obrigatória. Somente após finalizar o tempo de exibição é que o cliente terá total acesso à rede sem fio.

Obs.: Esta funcionalidade só é acessível no modo de operação "Roteador".

Splash page

Permite customizar anúncio para ser exibido nos dispositivos dos clientes antes de se autenticarem à rede Wi-Fi.

Tipo de Mídia Link da Mídia ⓘ

Vídeo (link da internet) https://

Tempo mínimo de visualização (segundos) ⓘ Tempo da Sessão ⓘ

30 30 minutos

Informações ao dispositivo conectado

Lista de SSID

Habilitado	SSID	Frequência	Tipo de Autenticação
<input type="checkbox"/>	AP3000AX_f1a8	Dual band	WPA2-PSK

SALVAR

- » **Tipo de mídia:** escolha entre um vídeo ou uma imagem
- » **Link da mídia:** informe o link da imagem ou vídeo. Para vídeos, apenas links dos sites "Vimeo" ou "Youtube".
- » **Tempo mínimo de visualização (segundos):** informe o tempo de visualização da mídia, em segundos. Tempo mínimo: 1 segundo. Tempo máximo: 120 segundos.
- » **Tempo da sessão:** informe o tempo máximo que o cliente pode ficar conectado na rede sem fio. Após o tempo finalizar, o cliente deve reconectar e visualizar a mídia configurada novamente. Mínimo: 1 minuto. Máximo: 60 dias.
- » **Informações ao dispositivo conectado:** Texto a ser exibido ao usuário após o encerramento do tempo mínimo de visualização da mídia. Caso este campo seja informado, o acesso total à rede sem fio só é concedido após a visualização da mídia e a confirmação da leitura deste texto.
- » **Lista de SSIDs:** Selecione as redes sem fio que exibirão a mídia configurada para visualização.

Discovery

Permite controlar a descoberta do produto na rede através de protocolos conhecidos.

Discovery

O discovery permite ao usuário fazer a descoberta dos equipamentos dentro da rede local, ou pela internet no caso de provedores.

☒ Defesa contra ataque de Força Bruta

☒ Protocolo LLDP

☒ Protocolo CDP

☒ Protocolo INTELBRAS

☐ Permitir Discovery na Interface WAN

SALVAR

- » **Defesa contra ataque de Força Bruta:** marque para ativar a proteção contra ataques de força bruta.
- » **Protocolo LLDP:** marque para permitir que o equipamento seja descoberto, através do protocolo LLDP.
- » **Protocolo CDP:** marque para permitir que o equipamento seja descoberto, através do protocolo CDP v1/v2.
- » **Protocolo INTELBRAS:** marque para permitir que o equipamento seja descoberto, através do protocolo Intelbras.
- » **Permitir Discovery na interface WAN:** marque para permitir que a função de Discovery passe a atuar na interface WAN.

NTP

Permite configurar os servidores que manterão o equipamento com data e hora atualizadas.

Data e Hora

O dispositivo mantém a hora certa a partir da sincronização com servidores NTP

☒ Habilitar cliente NTP

Servidor NTP 1
a.ntp.br

Servidor NTP 2
b.ntp.br

Zona
(GMT-03:00) São Paulo ▼

☐ Horário de verão

SALVAR

- » **Habilitar cliente NTP:** marque para manter o equipamento atualizado a partir dos servidores NTP informados. Para as configurações de "Agendamento", é necessário que esta configuração esteja ativa.
- » **Servidor NTP 1:** configure um endereço de servidor NTP primário. Servidores brasileiros são configurados por padrão.
- » **Servidor NTP 2:** configure um endereço de servidor NTP secundário. Servidores brasileiros são configurados por padrão.
- » **Zona:** Selecione uma das quatro zonas horárias brasileiras: "GMT-2", "GMT-3", "GMT-4" e "GMT-5".
- » **Horário de verão:** Selecione caso a sua localização adota o horário de verão.

SNMP

SNMP é um protocolo de comunicação usado em redes de computadores para monitorar e gerenciar dispositivos de rede. O SNMP permite que administradores de rede obtenham informações sobre o status e o desempenho desses dispositivos, além de configurá-los remotamente.

SNMP

Simple Gerenciamento de Dispositivos em Redes IP

☒ Habilitar SNMP ☐ Acesso via WAN

Comunidade

public

Porta SNMP

161

Localização

Intelbras - SC - Brasil

Contato

admin@meu_dominio.com.br

Nome

AP3000AX

SALVAR

- » **Habilitar SNMP:** marque para habilitar a visualização das informações transmitidas via protocolo SNMP.
- » **Comunidade:** informe o texto referente ao "SNMP Community".
- » **Porta SNMP:** informe a porta UDP de comunicação com o agente SNMP. Por padrão, a porta é 161.
- » **Localização:** informe o texto referente à localização.
- » **Contato:** informe o texto referente ao contato.
- » **Nome:** informe o texto referente ao nome desejado para o aparelho.

Watchdog

Função que reinicia o equipamento caso perca contato com um dispositivo da rede.

Watchdog

Temporizador para checar a comunicação com outros dispositivos

☒ Habilitar Watchdog

Endereço 1

192.168.1.1

Endereço 2

Domínio ou Endereço IP

Tempo de checagem (segundos)

30

SALVAR

- » **Habilitar Watchdog:** marque para habilitar a função "Watchdog".
- » **Endereço 1:** endereço IP ou domínio principal de um dispositivo na rede que será monitorado pelo equipamento. Caso perca contato e não houver endereço secundário configurado, o equipamento é reiniciado.
- » **Endereço 2:** endereço IP ou domínio secundário de um dispositivo na rede que será monitorado pelo equipamento. Caso não exista comunicação com o dispositivo primário, e também não obtenha comunicação com o secundário, o equipamento é reiniciado.
- » **Tempo de checagem:** informe o tempo de monitoramento dos endereços primário e secundário.

DDNS

DDNS é um serviço que permite associar um nome de domínio ao endereço IP endereço IPv4 público do equipamento. É fornecido suporte a três serviços DDNS: Intelbras, No-IP e DynDNS. Obs.: Esta funcionalidade só é acessível no modo de operação "Roteador".


DDNS

Permite associar um nome de domínio a um endereço IP

Serviço
Selecione ▼



Domínio
Domínio

Usuário
Usuário

Senha
Senha 

+ Criar DDNS

Domínios criados
Só é possível ativar um domínio por vez

☐ DynDNS - mypersonaldomain.dyndns.org
myusername  

Salvar

Para o serviço Intelbras DDNS:

- » **Domínio:** informe a primeira parte do domínio. **Obs.:** A parte final do domínio é fixa e inalterável: ".ddns-intelbras.com.br".
- » **E-mail:** informe o e-mail que receberá a confirmação da criação do domínio DDNS – Intelbras. O e-mail é encaminhado alguns minutos após a configuração ser aplicada.

Para o serviço "No-IP" e "DynDNS":

- » **Domínio:** informe o domínio configurado no site do serviço escolhido.
 - » **Usuário:** informe o configurado no site do serviço escolhido.
 - » **Senha:** informe a senha de acesso configurada no site do serviço escolhido.
- Obs.:** Para os serviços "No-IP" e "DynDNS", a confirmação da configuração deve ser feita no site do serviço escolhido.

Agendamento



Em "Agendamento" é possível planejar o ligamento das redes sem fio e dos LEDs. Na parte superior da tela é possível registrar agendamentos. Na parte inferior da tela é possível fazer a vinculação do agendamento com o funcionamento da rede sem fio (Wireless) e LED. Um mesmo agendamento pode ser vinculado tanto para o funcionamento das redes sem fio quanto para o funcionamento dos LEDs.



Agendamento

Adicione dias e horários para agendamentos

Tabela de Agendamentos

 ADICIONAR



Descrição	Dia da semana	Início	Fim	
Agendamento 1	Todos os dias	00:00	23:59	 

Linhas por página 6 1 - 1 de 1  

 WIRELESS LED

Agendamento Wireless

Habilitar	SSID	Agendamentos
<input type="checkbox"/>	AP3000AX_f1a8	Selecione

Linhas por página 6 1 - 1 de 1  

SALVAR

- » **Tabela de agendamentos:** informe a "descrição", os "dias da semana", "hora inicial" e "hora final" do funcionamento do agendamento.
- » **Wireless:** Aba para vincular o agendamento criado na "Tabela de Agendamentos" a uma ou mais redes sem fio.
- » **LED:** Aba para vincular o agendamento criado na "Tabela de Agendamentos" ao LED do produto.

LED

Configurações de funcionamento do LED do equipamento. Na configuração do LED é possível configurá-lo para permanecer desligado em todos os modos de operação. Há duas formas de configuração:

LED

Configurações do LED do roteador

Luz do LED

Configure a luz do LED do dispositivo

Sem suporte para esse dispositivo

Agendamento

Escolha um agendamento para luz de LED do dispositivo

Opção selecionada ▼

+ Criar novo agendamento

Localizar dispositivo

Ao acionar o botão, a luz do dispositivo piscará por 60 segundos

LOCALIZAR DISPOSITIVO

Cor da Luz do LED

Escolha uma cor para luz de LED do dispositivo

Sem suporte para esse dispositivo

Salvar

- » **Desligado:** LEDs permanecerão apagados.
- » **Programar horários:** configuração disponível caso existam agendamentos vinculados para o LED.

Segurança

Firewall

Restrição de acesso nas operações de transmissão ou recepção de dados.

Firewall

Restrição de acesso nas operações de transmissão ou recepção de dados

☒ Habilitar Firewall ☐ Habilitar ping na WAN ☒ Habilitar UPnP

Segurança

☒ Ativar todos

☒ Defesa contra ataque ICMP Flood

☒ Defesa contra ataque UDP Flood

☒ Defesa contra IP Spoofing

☒ Defesa contra ataque TCP SYN Flood

☒ Defesa contra escaneamento de portas / Flags inválidas TCP

☒ Defesa contra pacotes inválidos

SALVAR

- » **Habilitar firewall:** habilita o firewall.

- » **Habilitar ping na WAN:** desbloqueia o ping na WAN (disponível apenas quando em modo roteador).
- » **Habilitar UPnP:** habilita o Universal Plug & Play (disponível apenas quando em modo roteador).
- » **Segurança:** permite a ativação de defesas contra ataques e falhas conhecidas. (Ativadas por padrão)
- » **Defesa contra ataque ICMP Flood:** impede conexões ICMP de alto tráfego para o roteador ou através dele (aceita até 2/segundo com burst de 3).
- » **Defesa contra ataque TCP SYN Flood:** impede conexões TCP com flags FIN, SYN, RST, ACK/SYN de alto tráfego para o roteador ou através dele (aceita até 25/segundo com burst de 50).
- » **Defesa contra ataque UDP Flood:** impede conexões UDP de alto tráfego para o roteador ou através dele (aceita 10/segundo com burst de 20).
- » **Defesa contra escaneamento de portas/Flags inválidas TCP:** impede conexões TCP com flags FIN, SYN, RST, ACK/SYN de alto tráfego para o roteador ou através dele (aceita até 25/segundo com burst de 50).
- » **Defesa contra IP Spoofing:** impede conexões com IPs forjados/falsificados.
- » **Defesa contra pacotes inválidos:** impede transmissão de pacotes sem características válidas.

DMZ e Redirecionamento de Portas

Permite definir uma DMZ e também adicionar e remover regras de redirecionamento de portas.

Obs.: essa funcionalidade está disponível apenas quando o modo de operação for Roteador.

- » **Descrição:** descrição do controle.
- » **IP:** endereço IP destino.

Redirecionamento de portas (simples)

Controle de DMZ e Redirecionamento de Portas

Restrição de acesso nas operações de transmissão ou recepção de dados

Descrição

IP

Redirecionar Portas

Simples

ADICIONAR

Habilitar	Descrição	Intervalo de Portas	Protocolo	IP Destino
<input checked="" type="checkbox"/>			TCP/UDP	

Linhas por página

6


1 - 1 de 1

<

>

SALVAR

- » **Descrição:** descrição do controle.
- » **Intervalo de portas:** intervalo de portas a ser redirecionado.
- » **Protocolo:** selecione TCP, UDP ou TCP/UDP.
- » **IP de Destino:** endereço IP de destino.

Use o botão **+Adicionar** para criar as regras, ou use o botão  para excluir uma regra.

Redirecionamento de portas (avanzado)

Controle de DMZ e Redirecionamento de Portas
Restrição de acesso nas operações de transmissão ou recepção de dados

Descrição IP

Redirecionar Portas
Avançado ▾


 ADICIONAR

Habilitar	Descrição	IP / Rede Origem	Porta Origem	IP Destino	Porta Destino	Protocolo
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	TCP ▾ 

Linhas por página 6 ▾ 1 - 1 de 1  

 SALVAR

- » **Descrição:** descrição do controle.
- » **IP/Rede de origem:** define o IP/Rede de origem.
- » **Porta externa:** define a porta externa.
- » **IP interno:** define o IP interno.
- » **Porta interna:** define a porta interna.
- » **Protocolo:** TCP, UDP, TCP e UDP.

Use o botão **+Adicionar** para criar as regras, ou use o botão  para excluir uma regra.

Regras de firewall

Permite configurar regras de firewall avançadas, controlando tráfego com base em protocolo, endereço IP, rede e portas. Indicado para profissionais de rede experientes.

Obs.: essa funcionalidade está disponível apenas quando o modo de operação for Roteador.

Controle por MAC

Permite adicionar/remover regras de bloqueio ou liberação de acesso por endereço MAC.


Obs.: essa funcionalidade está disponível apenas quando o modo de operação for Roteador.

Regras de firewall

Configurações de firewall para permissões de tráfego na rede

CONTROLE POR MAC

CONTROLE POR IP

 BLOQUEAR TRÁFEGO

Descrição

Endereço MAC

+ CRIAR REGRA



Bloquear	Descrição	MAC
<input checked="" type="checkbox"/>	Dispositivo	A8:e3:ee:ba:ad:21 

Linhas por página 6 1 - 1 de 1 < >

SALVAR

» **Descrição:** descrição do controle.

» **MAC:** endereço MAC a ser bloqueado

Use o botão  **Adicionar** para criar as regras, ou use o botão  para excluir uma regra.

É possível habilitar ou desabilitar o bloqueio através da ação bloquear localizada na tabela onde são apresentadas as regras.

Controle por IP

Permite adicionar/remover regras de bloqueio ou liberação de acesso por endereço IP.

Obs.: essa funcionalidade está disponível apenas quando o modo de operação for Roteador.

» **Tipo de Controle:** escolha entre Controle por IP ou Controle por Faixa de Rede.

Controle por IP

Regras de firewall

Configurações de firewall para permissões de tráfego na rede

Controle por MAC

Controle por IP

☐ Modo avançado

☒ Controle por IP
 ☐ Controle por Faixa

Liberar tráfego

Bloquear tráfego

Descrição

Protocolo

TCP/UDP

IP / Rede

+ Criar regra

Habilitar	Descrição	Ação	Protocolo	IP / Rede
Nenhuma regra de firewall cadastrada				

Salvar

- » **Liberar tráfego / Bloquear tráfego:** define se a regra que será criada será para liberar ou bloquear o endereço IP informado.
 - » **Descrição:** descrição do controle.
 - » **Protocolo:** permite selecionar o tipo de protocolo que será realizado o controle da rede.
 - » **IP/Rede:** endereço IP ou faixa de rede a ser bloqueado ou liberado, bem como a máscara de sub-rede.
- Use o botão **Adicionar** para criar as regras, ou use o botão para excluir uma regra.

Uma vez a regra criada é possível editar sua descrição, ação, protocolo e também o IP/Rede definidos.

É possível habilitar ou desabilitar as regras através da ação Habilitar localizada na tabela onde são apresentadas as regras.

Controle por faixa

Regras de firewall

Configurações de firewall para permissões de tráfego na rede

CONTROLE POR MAC

CONTROLE POR IP

☐ Modo avançado

☐ Controle por IP
 ☒ Controle por Faixa

LIBERAR TRÁFEGO

BLOQUEAR TRÁFEGO

Descrição

Protocolo

Origem
 Endereço IP

Destino
 Endereço IP

+ CRIAR REGRA

Habilitar	Descrição	Ação	Protocolo	IP Inicial	IP Final
<input checked="" type="checkbox"/>	Teste	Liberar	TCP/UDP	192.168.1.1	192.168.1.254

Linhas por página 6 1 - 1 de 1

SALVAR

- » **Liberar tráfego / Bloquear tráfego:** define se a regra que será criada será para liberar ou bloquear o endereço IP informado.
 - » **Descrição:** descrição do controle.
 - » **Protocolo:** permite selecionar o tipo de protocolo que será realizado o controle da rede.
 - » **IP inicial:** endereço IP que inicia a faixa de IP a ser liberada ou bloqueada.
 - » **IP Final:** endereço IP que finaliza a faixa de IP a ser liberada ou bloqueada.
- Use o botão **+Adicionar** para criar as regras, ou use o botão **Excluir** para excluir uma regra.

Uma vez a regra criada é possível editar sua descrição, ação, protocolo e também o IP/Rede definidos.

É possível habilitar ou desabilitar as regras através da ação Habilitar localizada na tabela onde são apresentadas as regras.

Modo avançado

Estas configurações exigem um grau avançado de conhecimento sobre redes.
Apenas altere as opções de tráfego se tiver consciência dos efeitos em sua rede.

Regras de firewall

Configurações de firewall para permissões de tráfego na rede

CONTROLE POR MAC

CONTROLE POR IP

☒ Modo avançado

Estas configurações exigem um grau avançado de conhecimento sobre redes. Apenas altere as opções de tráfego se tiver consciência dos efeitos em sua rede.

LIBERAR TRÁFEGO

BLOQUEAR TRÁFEGO

Descrição

Protocolo
 TCP/UDP

Origem

☐ Exceto IP / Rede

☐ Exceto Porta

Destino

☐ Exceto IP / Rede

☐ Exceto Porta

+ CRIAR REGRA

Habilitar	Descrição	Ação	Protocolo	Origem	Destino
Nenhuma regra de firewall cadastrada					

SALVAR

- » **Liberar tráfego / Bloquear tráfego:** define se a regra que será criada será para liberar ou bloquear o endereço IP informado.
- » **Descrição:** descrição do controle.
- » **Protocolo:** permite selecionar o tipo de protocolo que será realizado o controle da rede.
- » **IP/Rede e porta de origem:** endereço IP/Rede e/ou Porta a rede a ser liberado ou bloqueado. Podendo ser definido uma exceção para a regra. Ou seja, aplicar a todos menos o IP/rede e/ou porta definida.

» **IP/Rede e porta de destino:** endereço IP/Rede e/ou Porta a rede a ser liberado ou bloqueado. Podendo ser definido uma exceção para a regra. Ou seja, aplicar a todos menos o IP/rede e/ou porta definida.

Use o botão **➕Adicionar** para criar as regras, ou use o botão **🗑️** para excluir uma regra.

Uma vez a regra criada é possível editar sua descrição, ação, protocolo e também o IP/rede e/ou porta de origem e de destino definidos.

É possível habilitar ou desabilitar as regras através da ação Habilitar localizada na tabela onde são apresentadas as regras.

Conexões

Dispositivos conectados

Permite acessar informações sobre os clientes conectados via Wi-Fi ou rede cabeada.

Dispositivos conectados
Informações sobre os clientes conectados via Wi-Fi ou rede cabeada

Interface: SSID: Tipo:

Pesquisar dispositivos
🔍 Digite o SSID, hostname ou endereço MAC que você procura

Interface	SSID	Hostname	IP	Tipo	RX	TX	Endereço MAC	Sinal	Frequência	Tempo de conexão
Ethernet	-	Não identificado	192.168.1.1	Estático	-	-	F6:92:BF:97:94:1B	-	-	-

Linhas por página: 1 - 1 de 1

- » **Interface:** permite filtrar os equipamentos por interface: Wireless, Ethernet ou Qualquer.
- » **SSID:** permite filtrar os equipamentos por SSID.
- » **Tipo:** permite filtrar os equipamentos pelo tipo: DHCP, Estático, Desconhecido ou Qualquer.
- » **Pesquisar equipamentos:** possibilita a busca de equipamento(s) por SSID, hostname ou endereço MAC.

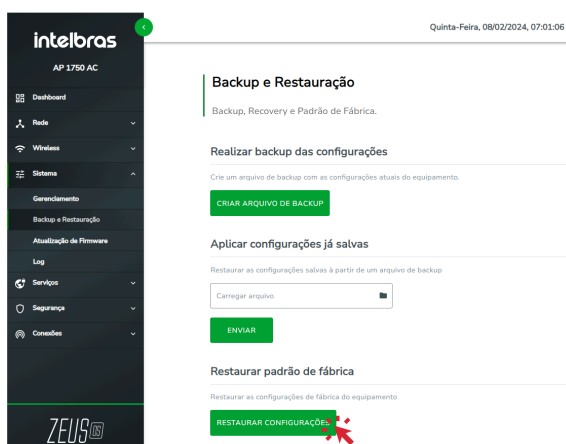
Reset (padrão de fábrica)

Há dois modos de redefinir as configurações:

- » **Botão reset físico:** Mantenha pressionado o botão Reset por aproximadamente 10 segundos. Solte-o e aguarde o equipamento reiniciar. O botão comumente se encontra na parte inferior traseira do equipamento.



- » **Reset via software:** use o botão Restaurar padrão de fábrica disponível na guia Sistema>>Configurações>>Configuração padrão de fábrica, na interface de gerenciamento web do produto.



Obs.: não desligue o equipamento durante esse processo.

Termo de garantia

Fica expresso que esta garantia contratual é conferida mediante as seguintes condições:

- » *Todas as partes, peças e componentes do produto são garantidos contra eventuais vícios de fabricação, que porventura venham a apresentar, pelo prazo de 1 (um) ano – sendo este de 90 (noventa) dias de garantia legal e 9 (nove) meses de garantia contratual –, contado a partir da data da compra do produto pelo Senhor Consumidor, conforme consta na nota fiscal de compra do produto, que é parte integrante deste Termo em todo o território nacional. Esta garantia contratual compreende a troca expressa de produtos que apresentarem vício de fabricação. Caso não seja constatado vício de fabricação, e sim vício(s) proveniente(s) de uso inadequado, o Senhor Consumidor arcará com essas despesas.*
- » *A instalação do produto deve ser feita de acordo com o Manual do Produto e/ou Guia de Instalação. Caso seu produto necessite a instalação e configuração por um técnico capacitado, procure um profissional idôneo e especializado, sendo que os custos desses serviços não estão inclusos no valor do produto.*
- » *Constatado o vício, o Senhor Consumidor deverá imediatamente comunicar-se com o Serviço Autorizado mais próximo que conste na relação oferecida pelo fabricante – somente estes estão autorizados a examinar e sanar o defeito durante o prazo de garantia aqui previsto. Se isso não for respeitado, esta garantia perderá sua validade, pois estará caracterizada a violação do produto.*
- » *Na eventualidade de o Senhor Consumidor solicitar atendimento domiciliar, deverá encaminhar-se ao Serviço Autorizado mais próximo para consulta da taxa de visita técnica. Caso seja constatada a necessidade da retirada do produto, as despesas decorrentes, como as de transporte e segurança de ida e volta do produto, ficam sob a responsabilidade do Senhor Consumidor.*
- » *A garantia perderá totalmente sua validade na ocorrência de quaisquer das hipóteses a seguir: a) se o vício não for de fabricação, mas sim causado pelo Senhor Consumidor ou por terceiros estranhos ao fabricante; b) se os danos ao produto forem oriundos de acidentes, sinistros, agentes da natureza (raios, inundações, desabamentos, etc.), umidade, tensão na rede elétrica (sobretensão provocada por acidentes ou flutuações excessivas na rede), instalação/uso em desacordo com o manual do usuário ou decorrentes do desgaste natural das partes, peças e componentes; c) se o produto tiver sofrido influência de natureza química, eletromagnética, elétrica ou animal (insetos, etc.); d) se o número de série do produto tiver sido adulterado ou rasurado; e) se o aparelho tiver sido violado.*
- » *Esta garantia não cobre perda de dados, portanto, recomenda-se, se for o caso do produto, que o Consumidor faça uma cópia de segurança regularmente dos dados que constam no produto.*

- » *A Intelbras não se responsabiliza pela instalação deste produto, e também por eventuais tentativas de fraudes e/ou sabotagens em seus produtos. Mantenha as atualizações do software e aplicativos utilizados em dia, se for o caso, assim como as proteções de rede necessárias para proteção contra invasões (hackers). O equipamento é garantido contra vícios dentro das suas condições normais de uso, sendo importante que se tenha ciência de que, por ser um equipamento eletrônico, não está livre de fraudes e burlas que possam interferir no seu correto funcionamento.*
- » *Após sua vida útil, o produto deve ser entregue a uma assistência técnica autorizada da Intelbras ou realizar diretamente a destinação final ambientalmente adequada evitando impactos ambientais e a saúde. Caso prefira, a pilha/bateria assim como demais eletrônicos da marca Intelbras sem uso, pode ser descartado em qualquer ponto de coleta da Green Eletron (gestora de resíduos eletroeletrônicos a qual somos associados). Em caso de dúvida sobre o processo de logística reversa, entre em contato conosco pelos telefones (48) 2106-0006 ou 0800 704 2767 (de segunda a sexta-feira das 08 às 20h e aos sábados das 08 às 18h) ou através do e-mail suporte@intelbras.com.br.*
- » Sendo estas as condições deste Termo de Garantia complementar, a Intelbras S/A se reserva o direito de alterar as características gerais, técnicas e estéticas de seus produtos sem aviso prévio.
- » Todas as imagens deste manual são ilustrativas.
- » Produto beneficiado pela Legislação de Informática.
Firefox é uma marca registrada da Mozilla Foundation. UPnP é uma marca registrada da UPnP Implementers Corporation.

Assinatura do cliente: _____

Fale Conosco

Termos de Uso

Política de privacidade

Suporte a clientes: (48) 2106 0006

Fórum: forum.intelbras.com.br

Suporte via chat e e-mail: intelbras.com.br/suporte-tecnico

SAC: 0800 704 2767

Onde comprar? Quem instala?: 0800 724 5115

Produzido por: Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira

Rodovia SC 281, km 4,5 – Sertão do Maruim – São José/SC – 88122-001

CNPJ 82.901.000/0014-41 – intelbras.com.br

Indústria Brasileira